CYBERTALK

Issue #4

Spring 2014

Produced with the kind support of

THE NATIONAL MUSEUM OF COMPUTING

ATTACK OF THE HIDDEN MENACE

INFECTED SUPPLY CHAINS!!

CORPORATE ESPIONAGE!!

INSIDER THREATS!!

Support ends for Windows XP and Office 2003.

Office 365

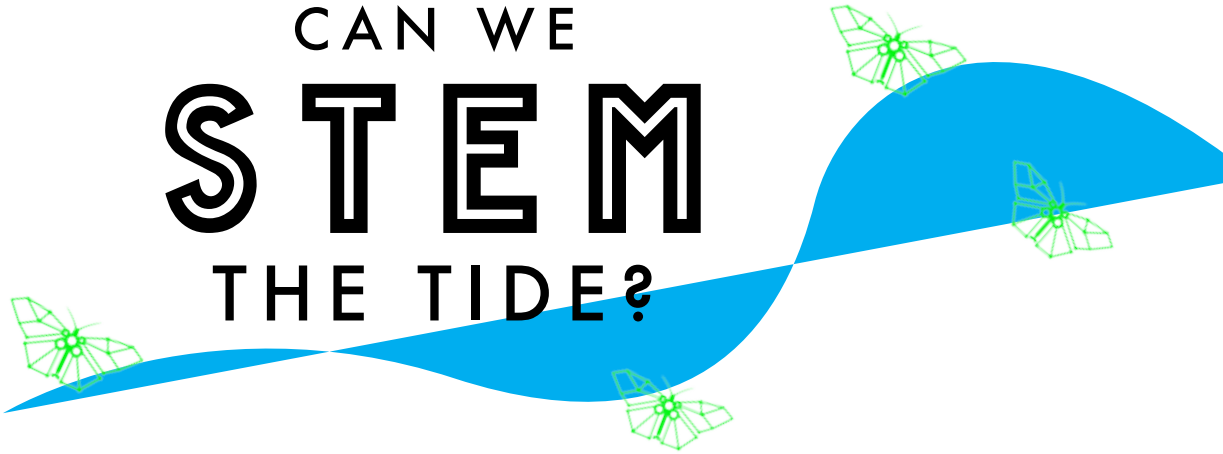
Windows 8 Pro

After April 8, 2014, there will be no more updates or support for Windows XP and Office 2003. These products were designed for a different era of technology and can no longer provide a secure technology foundation for governments, even with updates and anti-virus applications.

Find out how we can help you upgrade and save.
Call 01347 812100 or visit softbox.co.uk/microsoft

SBL™

CAN WE STEM THE TIDE?



By Colin Williams, Editor, Cybertalk

There is a longstanding commonplace amongst us, the community of cyber security experts, that the key to good cyber security tomorrow is to teach our children more and better science, technology, engineering and mathematics today. We have a common sense that we can STEM the tidal waves of the cyber security crisis. We are of the belief that if children can only be taught how to cut computer code then they will become good cyber citizens and cyber will be made safe. We lament with incredulity the idiocy of an approach that might teach our children how to use technology; how to behave in the cyber domain.

We express this view frequently and fervently at the many cyber security conferences we repeatedly attend. It is one of several that we particularly cherish. Another is that the controlling minds of the great institutions of our society and our economy are not taking the cyber security crisis seriously enough and so they must face the prospect of punishment if they persevere in their delinquency. Another is that users are somewhat stupid and even if they are not actually an active, insider, threat; then they are reckless and irresponsible in their desire to pervert our systems to their own uses. Another is that they, the users, the business, the children, must be educated out of their dangerous ignorance. Another is that there is a lack of a code of conduct for cyber, that cyber lacks normative behavioural standards.

These are the same conferences at which we have been gathering for over a decade. We have spent countless hours nurturing these commonplaces amongst ourselves; to ourselves. Countless hours exhorting our own community to 'beware' and to 'think very seriously about difficult problems'. Countless hours scaring ourselves with the magnitude and severity of the ever impending cyber apocalypse. Countless hours rehearsing slightly differing descriptions of the same problems; to ourselves. Countless hours showing each other how smart we are by showing off how easy it is for us, the experts, to break the systems we have designed. The systems we are responsible for securing.

These commonplaces are replete with contradictions and riddled with tensions. They have been repeated ad-nauseam with little or no regard to either the presence or the quality of available evidence. Our conferences have become episodes where we experts gather to console ourselves. They have long ceased to be crucibles of creative, structured, productive Socratic investigation. We must now subject our cherished commonplaces to the destructive and creative rigour that our status as experts demands of us. We must now start communicating, meaningfully, with those who are not us.

Cyber is a way of describing a system of profound complexity within which humans and machines interact and interoperate in new and transformative ways. Whatever good cyber security looks like, it is not reducible to technology and we cannot widget our way to human and societal safety in this new domain. As a community we will always default to a reliance on science, technology, engineering and mathematics. We think that because computers are machines then computing is simply a bigger machine. We are wrong. Computing is a human system. Computing is a social system. Computing has become the property of society. It is far too important to be left in the hands of technocrats. It belongs to them, not us. It's time to let the butterflies go.

CYBERTALK

CONTENTS

12

28

40

OFF TOPIC

Join the debate:

cybertalk@softbox.co.uk

@CyberTalkUK

Dear Sir,

Since the last Cybertalk, there has been an unprecedented and very welcome piece of news concerning the issue's subject, Dr Alan Turing. In December 2013, the wartime cryptanalyst and computer science pioneer was granted a Royal Pardon from his conviction of gross indecency.

Turing was convicted in 1952 after his homosexuality (illegal at the time) became known publicly. The consequences following his conviction were primitive, and it is widely believed that his treatment led to his emotional collapse and suicide. The government has previously declared regret for the way in which Turing was treated, with Gordon Brown apologising in 2009. However, this latest action goes much further and officially repeals Turing's conviction. This follows a long campaign from scientists including Stephen Hawking, and a petition to government with over 37,000 signatories.

For the government to have been so hostile to a man whose pivotal work took years off the Second World War, potentially saving millions of lives, has seemed irreparably unjust to many. Action like this can only be a gesture, but it aptly demonstrates the country's remorse and gratitude to an extraordinary man, without whom modern society would have been very different.

W.THOMASSEN (VIA EMAIL)

Dear Sir,

RE: MY LIFE AT BLETCHLEY - Henry Clifton's recollections of life at Bletchley Park after the war were fascinating, particularly his description of security (or lack thereof) at the base.

It is incredible to think that back then you didn't require any form of identification to enter such a facility. One can only imagine what hoops you would have to jump through to gain access to such a facility today.

L. BAHRAM (VIA EMAIL)

Dear Sir,

With the news that hackers have managed to crack an iPhone controlled lavatory (@CyberTalkUK, 05/08/13), the real question must surely not be "How did they do it?" but "Why would they bother?"

C. NORTHFIELD (VIA EMAIL)

TWEETS

"@CyberTalkUK Fantastic to see McAfee investing in Bletchley Park to develop and preserve the site for future generations."

@corrinadalby

➢ | CT. - We couldn't agree more - find out more from McAfee on p.26

@CyberTalkUK has interactive version of this superb #Turing Year special edition at www.softbox.co.uk/cybertalk. Lots of #BPark relevant info"

@AlanTuringYear

"I've been published for the first time! Ridiculously excited. The Enigmatic Alan Turing, p6 @CyberTalkUK"

@TomHook10

➢ | CT. - And he was so good we asked him back! Read "From 3D printers to Nanofactories" by Tom on P.36

SBL

EDITORS
Prof. Tim Watson
Colin Williams

ART DIRECTOR AND DIGITAL EDITOR
Andrew Cook

CHIEF SUB-EDITOR
Natalie Murray

CREATIVE PUBLICATION SPECIALIST
Tineke Simpson

CONTRIBUTORS
Prof. Alison Attrill
Prof. Martin Bateman
Ria Biggs
Hugh Boyes
Ian Bryant
Scott Cattaneo
Andrew Cook
Lucas Donato
Steven Holdway
Tom Hook
Dr. Andre Ara Karmanian
Max King
Roy Martin
Dr. Char Sample
Dr. Dan Shoemaker
Prof. Tim Watson
Colin Williams
Dr. Carol Woody

SPECIAL THANKS
The National Museum of Computing

DESIGN
Reflect Digital
www.reflectdigital.co.uk

CONTACT US
General enquiries:
+44 (0) 1347 812150
Editorial enquiries:
+44 (0) 1347 812100

Email: *cybertalk@softbox.co.uk*
Web: *www.softbox.co.uk/cybertalk*
Facebook: */cybertalkmagazine*
Twitter: *@CyberTalkUK*

Established in 1987 with a headquarters in York, SBL are a Value Added IT Reseller widely recognised as the market leader in Information Security. SBL offers a comprehensive portfolio of software, hardware, services and training, with an in-house professional services team enabling the delivery of a comprehensive and innovative range of IT solutions.

CyberTalk is designed by Reflect Digital and printed by Wyndeham Grange Ltd.

UK Government Releases iOS 7 Guidance

"Finding the right balance between security and usability is critical for all organisations."

SBL™

Authorised Reseller

In March 2011 the Government published the Government ICT Strategy. A major area of focus for the ICT Strategy is that of end user devices, with over 600,000 being employed across central government, and the Government End User Device Strategy, a sub strategy of the ICT Strategy, was released in October 2011.

The End User Device Strategy has been defined collaboratively by the End User Device Strategy subgroup, comprising representatives from Cabinet Office, Department of Health, Department for Work and Pensions, Government Procurement Service (now Crown Commercial Service), HM Revenue & Customs, Home Office, Ministry of Defence and Ministry of Justice. It has also been aligned to the wider ICT strategy, specifically the Public Services Network (PSN) and G-Cloud, where close dependencies exist.

The End User Device Strategy calls for Government access to the right tools to increase the productivity, flexibility and mobility of the public sector workforce.

"Consumer end user devices*, delivered to a clear standard that meets government needs, will maximise the productivity of the public sector workforce."

Building on the Cabinet Office's End User Device Security Framework, CESG, the Information Security Arm of GCHQ, has released security guidance to provide advice to those deploying devices by providing details on how particular platforms can be configured to achieve the key security recommendations contained in the Framework.

The online guidance is designed to help UK public sector security architects, system administrators and end-users as they deploy and use the latest laptops, desktops, tablets and smartphones.

The guidance also contains good practice advice on system architectures for remote and mobile working; details of particular configuration choices for each platform; and notes particular security risks and issues that organisations need to be aware of.

A senior cyber security expert at GCHQ said:

"Finding the right balance between security and usability is critical for all organisations and we have put this principle at the heart of our work. This guidance is the result of close collaboration between CESG's cyber security experts, our partners in industry and the public sector. It provides an excellent set of recommendations for anyone trying to enable secure business using the latest technologies in a cost-effective way."

CESG's guidance provides straightforward configuration advice for a range of devices and seeks to take a balanced approach between security and usability for remote or mobile working devices; helping to reduce common risks to an organisation's information whilst still providing the flexibility and ease of use required.

Liam Maxwell, the UK Government's Chief Technology Officer said of the guidance:

"This is precisely the sort of approach to security we need - simple, pragmatic, understandable."

SBL and Apple would like to bring to your attention that in January 2014, CESG released its security guidance on iOS7 and 7.1.**

iOS 7, launched September 2013, is Apple's most advanced mobile OS yet, including many new features designed to make it easier for businesses to put iOS devices in the hands of employees. Features such as better protection of work and personal data, management of app licences, seamless enrolment in Mobile Device Management, wireless app configuration, enterprise single sign on support and default data protection for third party apps.

Watch the video here: *http://www.apple.com/uk/ios/includes/videos/features.html#video*

Businesses around the world are choosing iOS devices for their enterprise-ready features. With a comprehensive approach to security, scaleable deployment options and a powerful platform for apps, iOS offers companies and organisations of all sizes just about everything they need to be more productive than ever.

The CESG guidance includes:

- Summary of platform security
- Significant risks
- How the platform can best satisfy the security recommendations
- Recommended network architecture
- Deployment process
- Provisioning steps
- Policy recommendations, and
- Enterprise considerations

Download a copy at *https://www.gov.uk/government/publications/end-user-devices-security-guidance-apple-ios-7*

*Definition of end user devices: PCs, laptops, tablets, smart phones and other hardware that end users can use to interact with data and applications.

**This guidance is applicable to devices running iOS 7 and 7.1. This guidance was developed following testing performed on iPhone 5S and iPhone 5 devices running iOS 7.0.4. The document is an update of the previous iOS 6 guidance.

SOURCES

http://www.apple.com/uk/ios/what-is/
http://www.apple.com/uk/ios/business
https://www.gov.uk/government/publications/end-user-devices-security-guidance-introduction
https://www.gov.uk/government/publications/end-user-device-strategy

Find Out More:
CyberTalk@softbox.co.uk
www.softbox.co.uk/cybertalk

The Children of Colossus

COLIN WILLIAMS

A History of Computing from Bletchley Park to the Berlin Wall and Beyond...

The computers of the Information Age were born in the crucible of total war. From the outset, the modern electronic computer was a device of war, deployed by the nation state in the prosecution of the mission of survival and victory. The computers of the Cold War were likewise an intrinsic and indispensable part of the existential struggle that defined the twentieth century.

Buried deep within the confines of Bletchley Park, hidden by the horrors and secrecy of a second 'war to end all wars', a machine was created that would change the world as we knew it. Colossus.

While it would be decades before its name and achievements would become public knowledge, the computer that helped take down a dictator had already given birth to mankind's newest age – the Information Age.

From the huts of Bletchley to the bunkers of the Cold War, *The Children of Colossus* explores the development of the computer and the social, political and economic impact it has had the world over.

About The Author

Colin holds a BA and an MA in History from the University of York, is a Visiting Professor at De Montfort University, Leicester and Business Development Director of SBL. He is a member of the Information Assurance Advisory Council Community of Interest and regularly speaks, consults and writes on matters to do with information assurance, cyber security and business development.

COMING SOON

Dr. Char Sample & Dr. Andre Ara Karmanian

A DIFFERENT PERSPECTIVE ON ATTRIBUTION

Brazil, China, India, Mexico and Russia: what do these countries have in common? These countries, along with several other countries, have all participated in nationalistic, patriotic themed website defacements in response to perceived threats by adversaries and, coincidentally, these countries also score on the high end of Hofstede's power distance index (PDI).

Why should we consider looking at actions and behaviours through Hofstede's framework? During a multicultural studies class, a professor remarked how the locals of one country shared with her the fact that they could always recognise the American tourists. They explained it was in the way they walked, their posture, and the amount of distance they needed from those around them. When looking at cyber behaviours the question arises: if national origin can be determined by a person's kinetic behaviour, can national origin be determined by attack behaviour? Like tourists who telegraph their national origins: can hackers unwittingly unveil their national origins? Do cultural clues reside in attack behaviours?

The link between culture and thought has long been established. Additionally, war and war games are tailored to reflect adversary behaviours, and these behaviours are culturally influenced. If kinetic war behaviours can be culturally influenced, cyber war behaviours should also share this trait.

Culture is a term that is widely used; however, a standard definition appears elusive. Geert Hofstede provides a definition that is generally accepted: "the collective mental programming that distinguishes one group of people from another" (Hofstede, Hofstede and Minkov, 2010). Academia's adoption of Hofstede's work implicitly validates his definition.

'Mental programming' is part of the automatic thought process. This suggests that certain behaviours, specifically cyber behaviours, may be mentally programmed into the warrior, and this mental program may be culturally influenced.

Hofstede et al. (2010) defined six dimensions of culture and the values are operationalised for each dimension. The definitions for each dimension can be found in Hofstede's works. Space limitations result in the omission of the definitions.

The initial work, in examining cyber behaviours, relied on known, existing behaviours. Therefore, the initial studies used self-identified, nationalistic, patriotic themed website defacements. These defacements were first identified at www.zone-h.org.

The initial study simply identified countries that participated in this type of behaviour. The countries were grouped together and compared against the overall population through means testing. The results showed that countries with high PDI values and low collectivist values participated in these attacks. An incidental observation found that, countries on the opposing poles were more likely to be the victims of these types of attacks instead of participants. The incidental observation was casual, and lacked the rigour of an academic study.

A second study was structured to determine if a correlation existed between the number of attacks and the dimensional value. This study showed an increase in the number of attacks as the PDI value increased, the correlation was strong (0.681). When these attacks were correlated with collectivism, a strong correlation (0.6669) was also found. One other dimension, a short-term orientation, also showed a strong correlation (0.6331) between the number of attacks and the dimensional value.

Additional studies are planned that examine other behaviours, and this particular defacement. These studies will be used to examine the level of aggression, and perhaps determine if a relationship exists between kinetic action and these defacements. The ultimate goal is to determine if Hofstede's framework, that is used to anticipate behaviours in the corporate world, is applicable to the cyber realm.

This article is the first in a series of articles that will detail our progress and observations in pursuit of this line of research. This research has far reaching implications for cyber operations. By performing cross-discipline research and using statistical analysis as the evaluation tool, we believe that we may be able to extend existing profiles to go beyond observed behaviours into the realm of forecasting cyber behaviours and attributing attacks beyond the IP address.

mind the gap

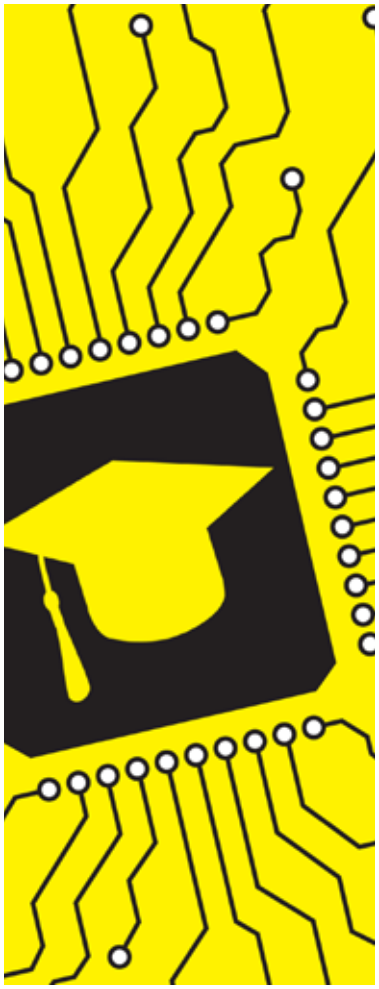
"COME MOTHERS AND FATHERS THROUGHOUT THE LAND
DON'T CRITICISE WHAT YOU CAN'T UNDERSTAND
YOUR SONS AND YOUR DAUGHTERS ARE BEYOND YOUR COMMAND
YOUR OLD ROAD IS RAPIDLY AGING
PLEASE GET OUT OF THE NEW ONE IF YOU CAN'T LEND A HAND
FOR THE TIMES THEY ARE A-CHANGIN"

BOB DYLAN – THE TIMES THEY ARE A-CHANGIN'

In 2013 a report by the National Audit Office (NAO) stated that the current IT skills gap in the UK could take more than 20 years to address, costing an estimated £27 billion a year and leaving the country's critical infrastructure extremely vulnerable to cyber-attacks.

With the shortfall estimated to be over 4.25 million people by 2015, Government ministers have since lead a recruitment drive to increase the amount of professionals entering the cyber domain. It has begun funding apprenticeships and trainee schemes, including one at GCHQ, and is also subsidising academics from Africa, Asia and America who will join Cranfield University's cyber policy course.

But is the industry in the dire straits we are lead to believe it is? There are already almost 100 UCAS accredited UK universities offering one or more Cyber security related degree courses (at all levels from BSc through to PhD), with the uptake of places very high across the board. Is the problem not so much the number of recruits wanting to take up roles in industry, but the recruitment process itself?



Speaking to Computing Magazine earlier this year, Professor Tim Watson believes there is no shortage of future cyber experts. "The high profile in the media that cyber has received recently, means that most people who are interested in a career in IT, computer science or related disciplines are aware of cyber. It's also quite glamorous, very fashionable and the salaries are very good," Watson said.

Yet increased financial constraints and a need for instant results mean that many companies are searching for the "perfect employee" – one with a mountain of experience yet willing to work for next to nothing. These are the candidates which do not exist. If the recruitment criteria was extended to afford greater investment and opportunity to interns and new graduates, would they surely not be repaid in triplicate in terms of energy, enthusiasm and new ideas?

Throughout this and subsequent issues of CyberTalk, students from across the UK's academic institutions, starting this issue with the Cyber Security Centre at De Montfort University, will demonstrate that the skills gap is not as wide as we're led to believe…

the danger of abstraction

BY STEVEN HOLDWAY
DE MONFORT UNIVERSITY

In the 1930s, Alonzo Church released his theory of a formal mathematical model (for expressing computation as a system of functions and substitutions) to the academic world in the form of lambda calculus.

However, despite the beauty and elegance of lambda calculus, a physical device that implemented it was impossible to build. It wouldn't be until many years later, and through the research and theories of Princeton fellows John Von Neumann and Alan Turing, that a device capable of digital computation would be built and pressed into service.

Now, just shy of a century later, we have advanced to the point where we can implement the principles of lambda calculus on stateful machines based on Von Neumann's architecture in the form of functional programming. What allows these two, fundamentally conflicting, models to work in harmony is layers of programmatic abstraction — abstraction that has long reached the sophistication where we can run virtual machines on top of physical ones and program in styles that fundamentally conflict with the physical machine underneath. Without reasonable abstractions, programmers would still be writing in binary and any hope of manipulating the machine in a functional manner would remain, just like the theory of lambda calculus, nothing more than a thought exercise.

Despite the importance of abstractions in computer science, the stacking of system upon system to build new platforms fundamentally clashes with one of the core principles of security-conscious programming: minimising the potential attack surface of the platform being developed. Modern smartphone operating systems are an excellent example of where it could be prudent to question the merit of placing abstractions on top of each other. The often cited 'modern computer in your pocket' analogy used to describe smartphones is not far off the mark. Android, as an example, features a complete GNU/Linux implementation, including shell and traditional userland, that exist far below the 'Dalvik' virtual machine and APIs typically utilised by Android application developers and core services. Despite being very capable, it is arguable that a smartphone platform does not benefit from an operating system and userland designed for much larger systems. The best case scenario is the unused features are simply bloat, the worst case scenario is that they are used as a vehicle for exploitation.

To give another example, prior to the BlackBerry 10 operating system and devices, the operating system that ran on BlackBerry phones was very tailored to the hardware, and to the planned functionality of the phone. The result, was a platform that was generally regarded as very secure, all while managing to retain a reasonable feature set. Unfortunately BlackBerry 10, now based on the QNX operating system, does not share its predecessors reputation for security; one of the first documented exploits (disclosed by SEC Consult) for BlackBerry 10 targeted the 'find' command-line utility that came with the QNX platform.

It becomes our task as security professionals, programmers, and computer scientists to start questioning the merit of layered abstractions in system design.

This raises the question of whether removing bloat and being more conscious about building abstractions upon abstractions should play a bigger role in the secure development lifecycle process. If the answer to this question is yes, then it falls to each development team's discretion of what is, and what is not, an acceptable level of risk in regards to abstractions.

To conclude, it becomes our task as security professionals, programmers, and computer scientists to start questioning the merit of layered abstractions in system design. Although building on previously built foundations gives notions of stability and security, we have to be careful not to end up with a tower of blocks that is a mere tap away from collapsing.

THE NATIONAL MUSEUM OF COMPUTING

INSPIRING FUTURE GENERATIONS AT THE

NATIONAL MUSEUM OF COMPUTING

The future is ever-present to anyone taking a tour of The National Museum of Computing located on Bletchley Park.

In one room alone the transition from the lonely monochrome prompt to the allure of the latest Touchtable is traced through 1980's BBC micros, interactive video, current laptops and the giant Domesday Touchtable of 2011. The thought that inevitably springs to mind is: Whatever will be next?

The National Museum of Computing is a inspirational resource for education. Schools are responding and last year 3,500 students aged from eight and upwards came for tours and taster classes in programming. Their enthusiasm is infectious with the result that teachers often want to book their next trip before they leave.

Young digital natives are astonished by the grand old machines like the rebuild of the 1944 Colossus and the 1951 WITCH and are mesmerised by the raw, naked and unreliable state of early pioneering computers.

"At the world-famous Colossus Rebuild we can address issues of online security," explained Chris Monk, Learning Co-ordinator at the Museum. "I can ask a student what his or her password is and as they start to blurt it out, I cut them short telling them that if they give their password away they aren't revealing just a little, but actually a huge amount. The single error of a Nazi operator of the Lorenz machine that enabled Tunny to be broken and Hitler's messages to be read puts that in vivid perspective."

"The WITCH is a particular favourite with teachers who are amazed that they can see the inner workings of a computer and explain to students through a working and very, very slow computer each processing stage with flashing lights and clattering relays."

Initially TNMOC was disappointed with the numbers of female students who came in the school groups, but even in the course of a little more than one year that seems to be changing. In January two groups from girls' schools came and were enthralled by what is too often seen as geeky boys' territory.

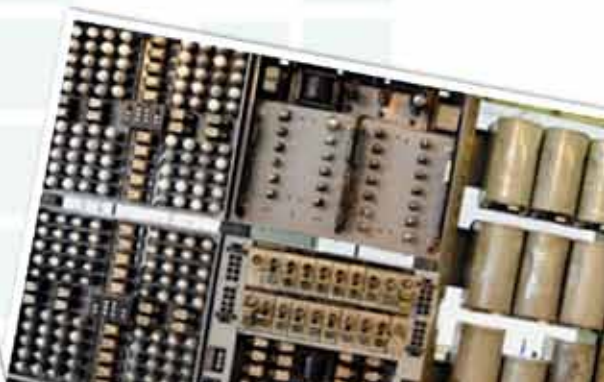
School groups come from far and wide, but many are able to stay long enough to have introductory coding lessons in the classroom lined with BBC micros.

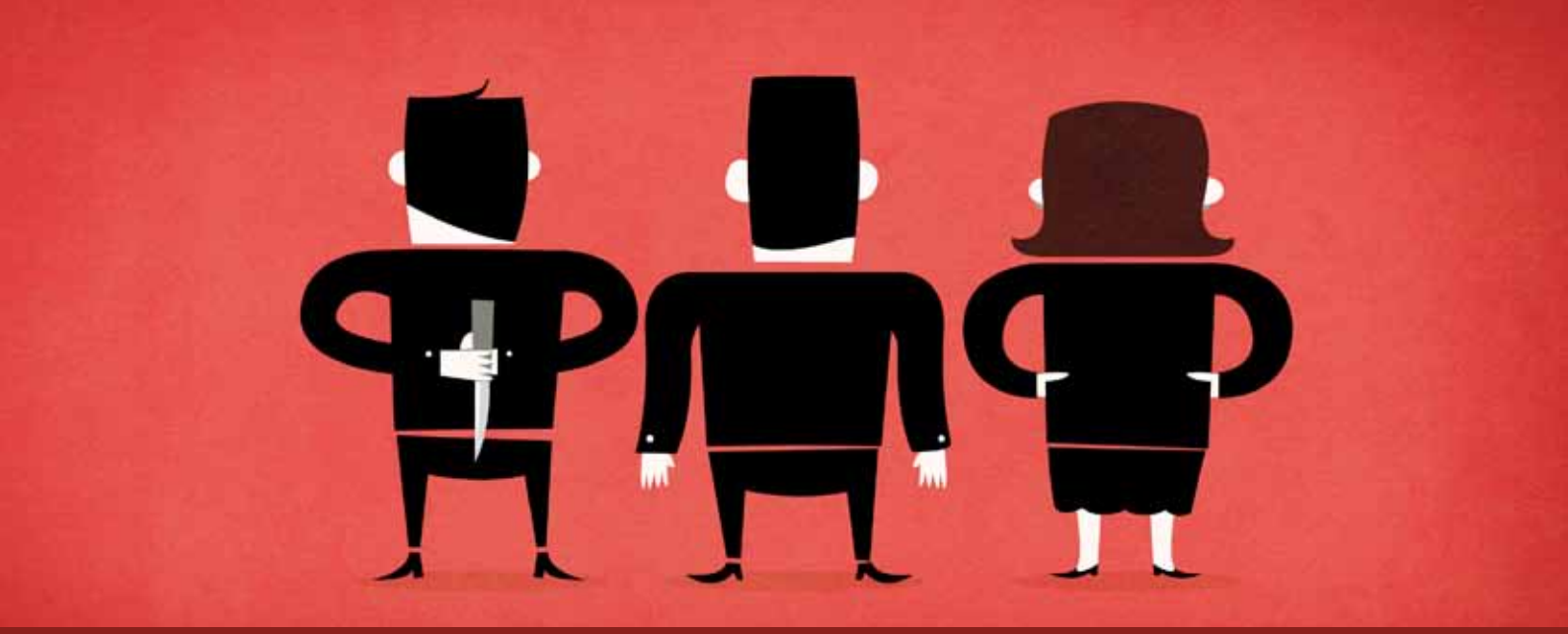
Chris Monk continued: "On almost every visit I hear teachers say: "The BBC got it so right." The BBC micro is an almost perfect teaching tool. Without any internet distractions and faced with an unfamiliar and seemingly scary screen prompt, it is actually very accessible and students rapidly gain confidence as they see how quickly they can start coding. It's great to see how creative and adventurous they quickly become. We have an increasing demand for take-home materials from pupils, students and teachers alike."

TNMOC is growing rapidly and learning on its feet as a pioneering museum now recognised as being world-class. In just two and a half years it has opened eight new galleries, each of which gives a fascinating insight of how quickly the world of computing has developed. The fact that this is all presented in historic Block H, the first purpose-built computer centre and home of Colossus, is not lost on visitors especially young people who get a particular buzz from that fact.

TNMOC opening times are increasing as funds become available. The Bytes Festivals during school holidays are an especially good time for families to visit. The Museum is not just for historians or those seeking nostalgia!

See www.tnmoc.org for more details.





What's On The Inside?

By Ria Biggs, *De Montfort University*

Often when information security mechanisms are implemented, it is the external attackers which we mostly look to prevent and detect. However, the 2011 Cyber Security Watch Survey[1] found 21% of attacks reported were by known or suspected insiders with 46% of respondents expressing concerns that the damage caused by insiders exceeded that of what external attackers could have caused. So why aren't we doing more to stop insider threats?

Insider threats have always existed. For some time we have been aware of the issue, confirmed in 1995 when Power[2] wrote "the greatest threat comes from inside your own organisation". However with our heavy reliance on rapidly advancing technologies, the insider threat continues to be a growing problem.

Many attempts have been made to define and characterise the insider threat over the years and these definitions have had to transform with advances in technology. Recently CERT[3] conducted a vast amount of research on this topic, resulting in a thorough definition featuring the key phrases; "authorised access", "intentionally exceeded or misused" to "negatively affect".

Unsurprisingly, the effect of insider activity can be far-reaching. Whether these activities are committed for revenge, financial or egotistical motivations, the consequences are the same. Damage is caused. This could be in the form of reputational damage, financial implications or physical damage to networks and equipment. Often, the scale of damage caused is even larger than that which could be caused by external attackers, and due to the authorised nature of insiders, it can often be undetected for longer periods of time.

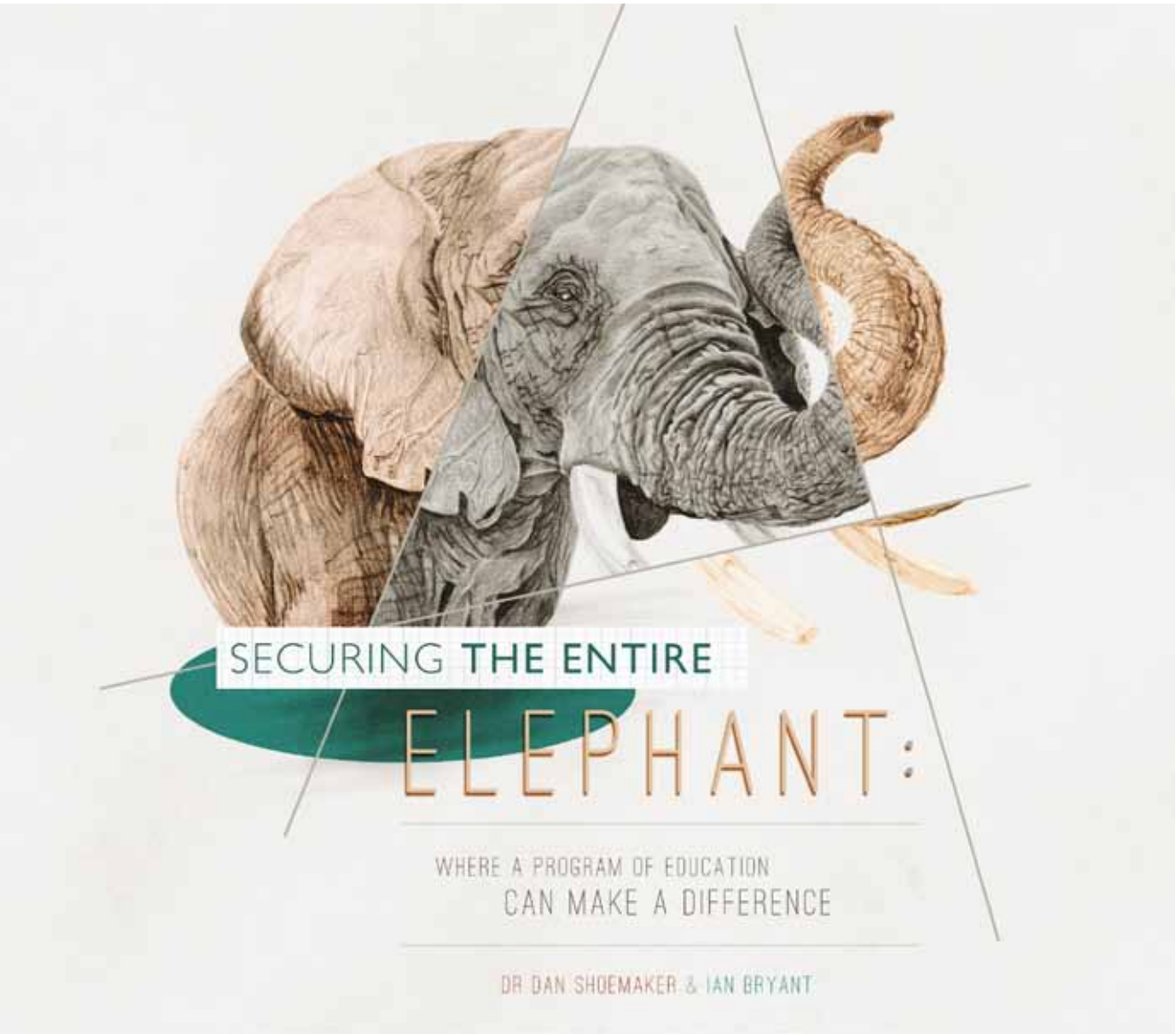
With the recent press attention surrounding Chelsea Manning (formerly Bradley Manning) and Edward Snowden, there is a concern that these detailed reports may expose the loopholes in technology systems which insiders often exploit. This may encourage the development of new insider threat actors as they become aware of the simplicity and effectiveness of conducting these detrimental activities.

A further concern is that our highly interconnected society, with a growing reliance on social media, could encourage a new type of insider threat; where social media profiles are used for the recruitment of organisations' employees by external groups. Alternatively, the nature of sharing on social media networks may encourage a generation of insider threats who share stolen data with their online network. Therefore, as the workforce becomes saturated with the tech-savvy generation Y, perhaps our concerns shall grow further.

Although an increasing problem, there has yet to be a successful and all-encompassing solution available for the prevention and detection of insider threats. Instead there continues to be many niche contributions to the area for both technological and behavioural detection mechanisms, each of which approach the problem at a different angle. This does not provide complete coverage for detection of the insider threat. Therefore, my contribution to this area as part of my final year project is the development of a prototype tool, which aims to detect insider threats by relying on artefacts that remain on a Windows host following the malicious activities. The tool is designed to focus on insider threat detection on the host machine alone; functioning to extract Registry data which relates to insider threat activities, to allow for the calculation of the likelihood that the user is an insider threat. The module currently developed for this prototype extracts Registry data regarding USB devices, to understand their activity on the host as they could potentially be utilised to steal or destroy data.

To conclude, it is hoped in the near future we will be able to combine many of our proposed insider threat detection solutions and provide an answer to the question – 'what's on the inside?'

1. CERT (2011) 2011 CyberSecurity Watch Survey – How Bad is Insider Threat? [WWW] CERT. Available from: www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf
2. POWER, R. (1995) Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare. California: Computer Security Institute.
3. CERT (2012) The CERT Insider Threat Center [WWW] CERT. Available from: http://www.cert.org/insider_threat/



The global economy rests on a technology base. So, it is common sense to make certain that that technology is secure. Sadly, current data from almost any source indicates that our systems are not secure.

The principal cause seems to be what might be called the "Six Blind Men and the Elephant" syndrome. In that old story six blind men are asked to describe an elephant based on what they are touching. So to one it's a snake, to another a wall, and to another a tree, etcetera. In the end, "Though each was partly in the right, all were entirely wrong". We have the same problem with cybersecurity. There are established elements of the field that know how to secure the part of the technology that they touch. But until we are able to coordinate that knowledge to secure the whole elephant, we can't realistically say we are secure. Or in pragmatic terms, "partly" secure simply does not suffice. Probably the best illustration of that old adage is the U.S. National Security Agency, which was done in by an insider exploit, not the electronic one that they were set up to prevent. This is where formal education comes in. Education shapes behaviour. For that reason, education can be an extremely powerful force for ensuring correct practice. Also, it is education's historical impact on society at large that makes it the most likely place to address the need for comprehensive cybersecurity.

Nevertheless, there are a number of challenges that have to be overcome. First, according to a report from the National Academies of Science, cybersecurity is an emerging discipline. Consequently, it is not clear what should be taught. Worse, all evidence points to the fact that whatever we should be teaching is cross-cutting. In essence, elements of the discipline could be taught in places as diverse as engineering, business, and law. These are different academic cultures, and cybersecurity practice is viewed differently in each. This cultural difference also raises the question of "to aggregate, or not to aggregate". If we leave the teaching of cybersecurity practice in diverse places on campus, we are not going to be able to coordinate the message, let alone evolve the field into a mature discipline. However, if we pull all of the cybersecurity education into a single place that begs the question of "where should we put it?", since engineers will not be comfortable in a law school and vice versa.

The term "holistic" has been used to describe what has to happen in order for the solution to be complete and correct. But the problem is that most present faculty members specialise in some vertical aspect of the discipline of computing. They are not going to just drop what they are teaching and start approaching things holistically. So, a new breed of professional will have to be educated. That returns us to the question of what to teach.

It should be obvious that a broad-scale development strategy based on a comprehensive definition of the field is needed to address the problem. That strategy should ensure that the right learning experiences are provided to the right people, across the educational landscape. However, effective strategy requires understanding the status of the existing landscape. Current cybersecurity teaching encompasses three classic domains. Those are, in order of formality, Awareness, Training and Education. A fourth area is the Research activity that supports all domains. Each domain can involve systematic, curricular or programmatic schemes, as well as unsystematic, "ad-hoc" efforts. Finally, there are a range of communities of interest where security teaching and learning might apply. Those 17 settings are listed in the table at the end of this article.

Awareness can be both programmatic and ad-hoc. Awareness is a very useful mode of content delivery in that it can ensure a minimum level of correct practice among a wide range of people. Formal awareness programs such as DHS Stop-Think-Connect utilise established methods for disseminating general knowledge such as posters, presentations and commercials. Informal programs include any educational activity sponsored by an organisation or group. The practices themselves can be relatively simple, such as secure housekeeping, phishing avoidance, or secure passwords. The messages themselves are often boiled down to slogans or sound bites.

Training can be formally sponsored, even certified. Training can be formal or organised to address a specific problem. Training is focused on the acquisition of a particular skill. That skill can be complex, like network administration, or secure programming. But training is always time sensitive in that the skills being provided can be made obsolete by change. Formal training programs, particularly those associated with certification, are based on commonly accepted bodies of knowledge. The end result of a training program is demonstrated mastery of that body of knowledge. Ad-hoc training provides mastery of a skill that might be required for a given application, or setting. Ad-hoc training is often deployed as corrective action, or in order to plug a knowledge gap in a particular instance.

Education can be programmatic and curricular, or it can be general. Programmatic education seeks to provide a reasoned understanding of a discipline or field. That understanding must be comprehensive in that the individual is capable of developing a heuristic solution from a given set of facts. Education is not time sensitive in that the educated individual should be capable of applying existing knowledge by extension to new problems. Because that capability often requires acquisition of a large amount of knowledge, programmatic education is decomposed into logical elements. This collection of elements is normally called a "curriculum". General education is not discipline specific. It can display the same characteristics of curriculum-based education in that it provides comprehensive and extensible understanding. However, general education is not directed toward mastery of a particular field.

Finally, Awareness, Training and Education activity is supported by research. Research develops knowledge and refines practice. There are two types of research programs. The first is practitioner-based research, aimed at developing useful skills and techniques. The second type of research is scientific in that it generates and confirms the correctness of new knowledge. This type of research can be unapplied but it is valuable because it forms the basis for the principles of the field.

If the aim is comprehensive cybersecurity then some form of all of these teaching modalities is required in all of the classic areas of society, government, industry and academia. Because the cultures of each of these communities are so different, the awareness, training and education needs vary across communities. That is an important point to keep in mind in developing any strategy aimed at ensuring cybersecurity. That is because content in any modality must be tailored to the community of practice in order to be effective. The table below shows all of the modalities we have discussed arrayed against the 17 logical communities of practice.

The question is, "How much of this table is blank?" In order for information system security to become a mature discipline every cell in this table should have some activity taking place within it or a reasonable justification for why that is not happening. Looking at this table it is hard not to conclude that we have a considerable way to go before we can say that we have gained control over the problem. It also tends to reinforce the conclusions of the National Academy of Science's findings, which is that the field is still immature.

Daniel P Shoemaker, PhD, Principal Investigator and Senior Research Scientist at UDM's Center for Cyber Security and Intelligence Studies. This Center includes the Computer Information Systems-Information Assurance Department, as well as the NSA Center of Academic Excellence in Information Assurance Education. As the Co-Chair for the DHS National Workforce Training and Education Initiative for Software and Supply Chain Assurance, he is one of the three Authors of the Software Assurance Common Body of Knowledge (CBK).

	Research Practitioner	Research Theorectical	Education Curricular	Education Ad-Hoc	Training Program	Training Ad-Hoc	Awareness Program	Awareness Ad-Hoc
GOVERNMENT								
National Security								
Conventional Agencies								
Contractors								
Aquisition								
INDUSTRY								
Government Supply Base								
Conventional Developers								
IT Sustainment								
Aquisition								
General Workforce								
INDUSTRY								
K-12								
Community Colleges								
Proprietary (for profit)								
College Undergraduate								
University Undergraduate								
College Graduate								
University Graduate								
Post Grad								

SECURITY THROUGH ASSUMPTION

MAX KING
Freelance Web & Mobile App Developer

You've had a brilliant idea for a new business and require a website, however lack the comprehensive security knowledge to build it yourself. Who do you hire?

Even though I have been a freelance programmer for 5 years I could count all the clients I have met face to face on one hand. That is because 90% of my work is obtained through intermediary companies that connect freelancers with clients across the globe. As convenient and helpful as it is to have access to such a large marketplace, it also means I am competing with people of all skill levels across international borders. I need to earn X a month, but my competitor who is also bidding on the same project may require much less due to favourable exchange rates, lower costs of living in their country and other such factors. I often find my bids undercut by ridiculous amounts and of course there is a trade off between expertise and price. These "cheap" bidders are who many will blame for the lax security on your newly built website. "Well, if you had paid a little more you wouldn't have these loop holes". But that is just not the case!

Of course there is a cut off point at which anyone with common sense should realise will yield inadequate and insecure programming. Your new website will contain endless amounts of personal data yet you set a budget of $10 USD an hour for a prospective programmer. Of course you will find someone to work on the project, but the quality of the security will not be top notch and worse possibly below the legal requirements. So you increase the hourly rate to $80 USD. Good, now you can assume that any applicant's abilities will be sufficient to keep your data secure. But how do you truly know? What questions do you ask a potential programmer to check their knowledge of securing data, if you yourself are relying upon them to secure your website properly?

On a weekly basis I am hired by sceptical website owners to perform code audits on their websites and to search for security vulnerabilities. I have come across websites that store passwords in plaintext, websites that do not cleanse or sanitise any user input they pass to a database and websites that allow the uploading of any file type and execution of said files. These websites are not just little hobby websites either, some have been websites with thousands of subscription paying members. On more than one occasion user's email addresses were stored next to a plaintext password, which I am certain if I had tried to use on their email account, the majority would have worked. Worst of all the website owners often have no clue of the gaping holes in their websites or the consequences of such simple mistakes. In their mind they have already paid for someone's expertise and that should have been sufficient to secure their websites data.

WEBSITE OWNERS OFTEN HAVE NO CLUE OF THE GAPING HOLES IN THEIR WEBSITES OR THE CONSEQUENCES OF SUCH SIMPLE MISTAKES.

There is another type of client I have come across that will hire me to add functionality. However I will always notify them if there are any obvious security holes in their websites I come across while working. To my amazement they will push that under the rug often saying "We can ignore that, please just add the functionality I requested."

This raises two fundamental questions. As the owner of a website with no technical know how, how can you be sure your website is secure? Equally as a website's end user, how can you be sure that the website you just passed your email address and password to are acting responsibly to secure the storage of them?

The first is not too hard as long as you are willing to spend that little more to hire a second independent party to audit the first's code. A simple, but effective remedy. This is the safest method to cover a new website as there is no universal standard or award to compare a programmer's ability to counter security threats. Of course they may have an accreditation for a specific language or database or even a computer science degree, but none of these are designed to focus solely and specifically on securing data. More importantly though when building a new website you combine multiple languages and technologies, so an accreditation in one does not necessarily cover their knowledge in another.

For the latter question though there is no satisfactory answer except to assume that you are using secure websites. Without an independent body to inspect a websites coding practices and storage techniques, we as end users must assume and hope that the data we provide is handled in the best manner that it can be.

TOP TIPS FOR HIRING A DEVELOPER:

- Check their previous work. This can sometimes be hard due to Non Disclosure Agreements, but they should be able to show something.
- Try to arrange a video conference or a phone call at the very least. This will help you to gauge the competency of a developer by asking questions they cannot rehearse and perfect their answers to.
- Do not commit the entire project from the start to one developer. If possible hire a prospective developer for a small portion of the project as a test of their ability and your working relationship.

Max King is a Freelance Web & Mobile App Developer, with a specific skill set laying in creating complex functionality. He worked part time under the guise of King Kreations before and throughout University to pay his fees, but upon graduation decided to commit himself full time. In the two years since then, Max has worked on more than 80 separate projects for individuals up to multinational corporations across all industries and all requirements. http://www.kingkreations.co.uk

CYBER SECURITY

Research Wiki

Scott Cattaneo – Commercial Manager, SBL

It gives me great pleasure to announce that SBL have embarked upon an exciting new project; the development and maintenance of a Cyber Security Research Wiki.

Recent collaboration with Academia and Industry both here and overseas has served to identify a clear and profound requirement for a central repository of useful and leading edge cyber security research, information, and best practice guidance material.

Many leading Academic Institutes publish research material, white papers, best practice documents etc. within their own domains or within their own communities. Some of these useful resources are more accessible than others (indeed much of this is public domain through various websites), yet it is clear that there is no single searchable area where practitioners can access this information as they seek to bolster their security in the wake of new Cyber threats.

A wiki is a very familiar and useful format for such a resource, and whilst we concede that the ability to include everything that could possibly be useful in this context would be an unsurmountable task, we do believe that through working with the various experts in our community we can get the best and most relevant content produced in a wiki that practitioners can reference and make excellent use of. This could be extremely useful both the public and private sector, could save countless hours of research time, and crucially will help organisations improve their security.

Working with our global Academic and Industry partners, SBL are in the process of coordinating a gathering of willing "Cyber Experts" to assist with the production, collation, vetting, and monitoring of Cyber Security Research Wiki content. As this team grows, the content will become more comprehensive, more innovative, and more diverse. Indeed it will improve exponentially as the collaboration extends and develops.

The wiki is interdisciplinary and the team behind the content will comprise leading experts from the key Academic institutes from around the world, as well as experts within the Cyber Security Industry.

The wiki has been built with some provisional content uploaded in the BETA version. We are now pleased to announce that we have entered the testing phase! Layered security is provided through the use of Digital Certificates, and we are now ready to engage you, the Cyber community and CyberTalk readership in this breakthrough common good initiative!

We hope you will all benefit from access to the content, and hope you will all be willing to provide constructive feedback which will help us to improve and develop this resource over time. Indeed, we hope we can identify some new collaborators out there, people who produce content that could be useful to the Cyber community in the on-going fight against our common threats and adversaries.

To apply for your free Digital Certificate which will provide "read only" access to the Wiki, please contact support@cybertalkwiki.co.uk.

You can also join the discussion on our Cyber Security Research Wiki LinkedIn page on http://ow.ly/tvbCe

We look forward to working with you to develop and deliver this new and exciting resource!

Redefining office IT. PowerEdge VRTX.

The first and only full integration of servers, storage, networking and management in only 5U.

Up until now, there hasn't been an IT solution designed specifically for an office environment. Enter the new Dell PowerEdge VRTX powered by the Intel® Xeon® processor, an integrated end-to-end solution built specifically for the growing office. It's the only 5U PowerEdge shared infrastructure platform design based on input from over 7,000 customers, featuring four integrated servers, 48TBs of storage, networking and systems management to simplify all aspects of IT. You inspired it. Dell built it.

The power to do more

Premier
Dell PartnerDirect Partner

Call 01347 812150
for a quote or email
Dell@softbox.co.uk

Find out about SBL's hardware solutions at http://www.softbox.co.uk/hardware

IACG: WORKING TO MAKE THE THE IA MARKET DELIVER FOR GOVERNMENT & INDUSTRY

The Information Assurance Collaboration Group (IACG) was formed following the National IA conference in 2006 ('IA06') to encourage greater collaboration between the commercial supply base for IA products and services operating within the UK public sector and the Wider Information Assurance Centre (WIAC) including specifically CESG and also including OCSIA, ICO & CPNI.

The key objectives of the IACG, on behalf of its members are to gain insight into the Government IA market; define IA as a market segment that delivers value to shareholders and customers; influence the UK IA market and align to overseas IA markets, and to help realise a position whereby the UK IA market is recognised as being world leading, in order to deliver competitive advantage for the UK supply base.

IACG has a 'special relationship' with CESG as its 'go to' organisation for independent Industry input, and the two organisations work closely through regular meetings and working groups to help CESG identify and remove barriers to the delivery of IA solutions for HMG, whilst also developing market conditions that encourage industry to innovate technically, and by influencing Government buying mechanisms for IA in order to encourage competitive market development. IACG can also explain common industry issues and concerns to CESG and facilitate communication across industry constituencies.

The governing principles of the group are that IACG does not engage in commercial activities or undertake any activity that may be construed as anti-competitive. It is also a consensus building group, and does not make any binding commitment on Members, all of whom offer resources & information on a voluntary and unpaid basis. Along with a 'Chatham House rule', freedom of expression is a major factor in ensuring that full and healthy debate of all IA issues is undertaken.

IACG frequently collaborates with other industry groups to avoid duplication and competition, and has worked with Tech UK, CDF, UKCeB, IAAC, BCS and CREST, amongst others, on numerous work packages providing practical outcomes on IA issues. More recently, IACG has also developed a close relationship with BIS, and has contributed to a number of work packages of mutual interest. BIS now has permanent representation at IACG meetings.

The BIS engagement is helping to build on the value already seen in collaboration with CESG, who recognise that IACG can help deliver improved quality, quantity and value in IA delivery, to both HMG and UK plc. In particular, CESG has expressed the value it sees in having a forum which is genuinely representative of Industry, with major Primes and micro SMEs having an equal voice, in which it can engage with Industry in constructive dialogue, and which has sufficient credibility and gravitas that it can genuinely influence the UK IA Industry through the group, as well as use it as an efficient forum for dissemination of information.

Key areas of current activity include Metrics, Organisational Standards and the HMG Classification Review. One of IACG's oldest and most popular products is the UK IA Community Map. This is an annual survey of all groups actively engaged on IA work and is now undergoing its fifth update, making it the most enduring and accurate survey of its kind. In recent years, SBL has provided the underpinning resource for collection and collation of the survey responses. The outputs of the survey are an annually published Map of the community, available via the CESG website at http://www.cesg.gov.uk/AboutUs/Pages/IA-Communities.aspx and a supporting contacts database, available on request to members. IACG is currently looking at options for transforming the map publication into a more interactive web service in order to provide greater value to both members and the wider IA community of interest.

Further information on IACG can be obtained from the Secretary, Joesph Taylor at Joseph.Taylor@techUK.org or for further information on the UK IA Community map, contact the Map Manager, Roy Martin at Roy.Martin@anneroy.co.uk .

PRINCIPLES OF SOFTWARE ASSURANCE

DR. CAROL WOODY
CARNEGIE MELLON UNIVERSITY

There are standards, practices, and methods to define what should be done to address software assurance, but no explanation of why it is needed in the first place. This set of principles assembled by a team of researchers at the Software Engineering Institute formulates a response to that need. This article is primarily an excerpt from "Foundations for Software Assurance" by Carol Woody and Nancy Mead of SEI, and Dan Shoemaker, University of Detroit Mercy and presented at the Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii 2012.

The full paper is available for your review at http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=75631.

Much of the information protection in place today is based on principles established by Saltzer and Schroeder in their paper "The Protection of Information in Computer Systems," which appeared in Communications of the ACM in 1974 [1]. They defined security as "techniques that control who may use or modify the computer or the information contained in it" and described the three main categories of concern: confidentiality, integrity and availability (CIA). Their proposed design principles, which focus on protection mechanisms to "guide the design and contribute to an implementation without security flaws" [1], are still taught in today's classrooms. They established eight principles for security in software design and development [1]:

1. Economy of mechanism: Keep the design as simple and small as possible.
2. Fail-safe defaults: Base access decisions on permission rather than exclusion.
3. Complete mediation: Every access to every object must be checked for authority.
4. Open design: The design should not be secret. The mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific, and more easily protected, keys or passwords.
5. Separation of privilege: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
6. Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
7. Least common mechanism: Minimise the amount of mechanism common to more than one user and depended on by all users.
8. Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Time has shown the value and utility in these principles; however, it is appropriate to consider that these were developed prior to the Morris worm that generated a massive denial of service by infecting over 6000 UNIX machines on November 2, 1988 [2]. To provide a technology context, consider that the IBM System 360 was in use from 1964–1978, and the IBM System 370 came on the market in 1972. An advanced operating system MVS (Multiple Virtual Storage) was released in March 1974 [3].

These principles were assembled prior to the identification of the more than 46500 software vulnerabilities and exposures that are currently exploitable in today's software products as described in the Common Vulnerabilities and Exposures (CVE) database at http://cve.mitre.org/. When these principles were developed, "buffer overflow," "malicious code," "cross-site scripting" and "zero-day vulnerabilities" were not part of the everyday vocabulary of operational software support personnel. Patches were carefully tested and scheduled to minimise operational disruption instead of pushed into operation to minimise attack vectors.

While these principles are still usable today in consideration of security within an individual piece of technology, they are no longer sufficient to address the complexity and sophistication of the environment within which that component must operate. We must broaden our horizon to consider the large scale, highly networked, software dependent systems upon which our entire critical infrastructure depends, from phones, power and water to industries such as banking, medicine and retail.

Software assurance is the commonly used term to describe this broader context. The Committee on National Security Systems (CNSS) [4] defines software assurance as follows:

"Software assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner."
There are vast lists of practices and procedures that describe what should be done to address software assurance. There are also an equal number of complaints that effective assurance is not being addressed in today's software. We posit that some of the inaction stems from a general lack of understanding about why this additional work is needed. In our scrutiny of the wide range of materials published, the case for why to focus on software assurance, a question any two-year-old would ask, has not yet been addressed. We propose the following seven principles in response:

RISK

A perception of risk drives assurance decisions. Organisations without effective software assurance perceive risks based on successful attacks to software and systems and usually respond reactively. They may implement assurance choices such as policies, practices, tools and restrictions based on their perception of the threat of a similar attack and the expected impact should that threat be realised. Organisations can incorrectly perceive risk when they do not understand their threats and impacts. Effective software assurance requires that risk knowledge be shared among all stakeholders and technology participants; however, too frequently, risk information is considered highly sensitive and is not shared, resulting in uninformed organisations making poor risk choices.

INTERACTIONS

Highly connected systems like the Internet require alignment of risk across all stakeholders and all interconnected technology elements; otherwise, critical threats will be missed or ignored at different points in the interactions. It is no longer sufficient only to consider highly critical components when everything is highly interconnected. Interactions occur at many technology levels (e.g., network, security appliances, architecture, applications, data storage, etc.) and are supported by a wide range of roles.

Protections can be applied at each of these points and may conflict if not well orchestrated. Because of interactions, effective assurance requires that all levels and roles consistently recognise and respond to risk.

TRUSTED DEPENDENCIES

Because of the wide use of supply chains for software, assurance of an integrated product depends on other people's assurance decisions and the level of trust placed on these dependencies. The integrated software inherits all of the assurance limitations of each interacting component. In addition, unless specific restrictions and controls are in place, every operational component including infrastructure, security software and other applications can be affected by the assurance of every other component. There is a risk each time an organisation must depend on others' assurance decisions. Organisations should decide how much trust they place in dependencies based on a realistic assessment of the threats, impacts and opportunities represented by an interaction. Dependencies are not static, and trust relationships should be regularly reviewed to identify changes that warrant reconsideration. The following examples describe assurance losses resulting from dependencies:

- Defects in standardised pieces of infrastructure (such as operating systems, development platforms, firewalls, routers, etc.) can serve as widely available threat entry points for applications.
- Using many standardised software tools to build technology establishes a dependency for the assurance of the resulting software product. Vulnerabilities can be introduced into software products by the tool builders.

ATTACKER

A broad community of attackers with growing technology capabilities are able to compromise the confidentiality, integrity and availability of an organisation's technology assets. There are no perfect protections against attacks, and the attacker profile is constantly changing. The attacker will use technology, processes, standards and practices to craft a compromise (known as a socio-technical response). Attacks are crafted to take advantage of the ways we normally use technology or designed to contrive exceptional situations where defences are circumvented.

COORDINATION AND EDUCATION

Assurance requires effective coordination among all technology participants. Protection must be applied broadly across the people, processes and technology in an organisation because the attacker will take advantage of all possible entry points. Authority and responsibility for assurance must be clearly established at an appropriate level in the organisation to ensure the organisation effectively participates in software assurance. This assumes that all participants know about assurance, and that is not usually a reality. There is much to be done to educate people on software assurance.

WELL PLANNED AND DYNAMIC

Assurance must represent a balance among governance, construction and operation of software and systems and is highly sensitive to changes in each of these areas. An adaptive response is required for assurance because the applications, interconnections, operational usage and threats are always changing. Assurance is not a once-and-done activity. It must continue beyond the initial operational implementation through operational sustainment. Assurance cannot be added later; it must be built to the level of acceptable assurance that organisations need. No one has resources to redesign systems every time the threats change, and assurance cannot be readily adjusted upward after the fact.

MEASURABLE

A means to measure and audit overall assurance must be built in. That which is not measured cannot be managed. Each stakeholder or technology user will address only the assurance for which they are held accountable. Assurance will not compete successfully with other competing needs unless results are monitored and measured. All elements of the socio-technical environment, including practices, processes and procedures, must be tied together to evaluate operational assurance. Organisations with more successful assurance measures react and recover faster, learn from their reactive responses and that of others and are more vigilant in anticipating and detecting attacks. Defects per lines of code, a common development measure, may be useful for code quality but are not sufficient evidence for overall assurance because they provide no perspective on how that code behaves in an operational context. Both focused and systemic measures are needed to ensure the components are engineered with sound security and the interaction among components establishes effective assurance.

Understanding why software assurance is needed increases the motivation to appropriately address the necessary practices, standards and methods that must be implemented to provide the desired assurance. The principles help everyone involved in software assurance understand its importance and value. Communicating them across the software development community is a critical next step.

ACKNOWLEDGMENTS

Copyright 2013 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

DM-0000828

REFERENCES

[1] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Communications of the ACM, vol. 17, issue 7, 1974.

[2] Wikipedia, "Morris worm," Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/Morris_worm. [Accessed June 2011].

[3] Wikipedia, "IBM System/370," Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/System/370. [Accessed June 2011].

[4] Committee on National Security Systems, "Instruction No. 4009," National Information Assurance Glossary. Revised June 2009.

OF BYTES AND BUNKERS

COLIN WILLIAMS, SBL

WE ARE THE EXPERTS.

We are the experts. The controlling minds of the institutions of the state, of society and the economy, and those who offer them sage counsel. The technocratic elite of computing, and of cyber security.

We are Generation X. Our grasp of the levers of power and influence is temporary, and we have been served our notice by Generation Y. These Millennials are impatient for control. We have a finite and diminishing period in which to contribute to the solution of the problems of our time and so control our legacy. Our context was forged during the Cold War. The world we made, the time and space we lived in, and the ways in which we sought to make sense of it all, were given their shape and form by a context. A context within which we were simultaneously subjects and objects; we made it as much as it made us.

We are beginning to apprehend the enormity of the transformations of the Information Age. Now, belatedly, we catch our first true glimpse of the gaping chasm separating us from the Millennials. We are easy prey to the collective paralysis of future shock. The symmetry, clarity, predictability and certainties of the Cold War appear comforting. A world of clear and certain binary choices; of absolutes of right and wrong. Of survival or total destruction. Bunkers of the mind are as real as those of steel and concrete. The one the tomb of the intellect as the other was the tomb of hope. The UK and US governments constituted the dominant protagonists in the NATO alliance, the anchor points of the economically and culturally dominant Atlantic axis, and the powerhouses of the post war development of computers. Across the span of the Cold War, US and UK government spending in general, and defence and intelligence spending in particular, dominated and shaped computing. The computers of the Cold War were an intrinsic and indispensable part of the existential struggle that defined the twentieth century. These governments spent according to their established patterns, within the dominant macro-economic structures of the age, and according to the imperatives of the Cold War.

The business of computing followed the pattern of the age. The supply chain for computers was vertically integrated. Narrow, short, and almost entirely knowable. Little of the work went beyond the commercial boundaries of the principal players and when it did, it did not stray far. The entire supply chain, should, and could, be mapped. From research and development, through to specification, implementation, testing, integration, operation and disposal; the system life cycle was predictable. The supply chain a part of the deterministic system as a whole. The idea of a complex matrix of volatile, recursive and nested sub contracts and outsourced obligations, if it occurred at all, would have been a nightmare of apocalyptic proportions.

The vertical integration of the sort common across the military industrial complex of the Cold War has gone. Outsourcing, globalisation, just in time disciplines, the emergence of what were once developing economies as principal actors in shifting patterns of geo-political power, have all converged to produce a supply context of bewildering complexity. The supply cartography of our context is essentially unknowable, partly because of its intrinsic and accumulated complexity, and partly because of its volatility. Whereas the commercial relationships of the vertically integrated constructs of the Cold War prized stability and longevity, those of the Information Age thrive on velocity. In the Machine Age we etched company names in stone, inscribed job titles in brass plates and kiln fired enamel adverts with retail prices emblazoned in ceramic permanence. Now, our advertising hoardings are computer monitors; facets of the cyber phenomenon. Our Millennial staff, entangled in patterns of loyalty utterly different to ours.

Cyber is about far more than computers and computer networks, however vast, far reaching and powerful they are. It is about far more than the Internet; whether of information or of things. It is about far more even than the laggardly realisation that the great interconnectedness of everything encompasses ICS and SCADA systems and, therefore, the totality of the critical infrastructure of every nation on earth. Humanity is existentially reliant upon cyber.

Micro fabrication will, within decades, destroy, disrupt and recreate entire swathes of economic activity; whilst creating entirely new ones. Our lack of understanding of the cyber supply chain is already scaring us and yet we only have a few years until computers will be manufactured in homes around the globe as easily as we now print off airline boarding passes. We have only begun to experience the first tingling of what will become abject terror at the prospect of the impact on structures of warranty, indemnity and liability of a supply chain where spare and replacement parts for critical systems are locally fabricated using binaries downloaded from the Internet and so utterly devoid of provenance or attestations of fitness for purpose.

NOW, BELATEDLY, WE CATCH OUR FIRST TRUE GLIMPSE OF THE GAPING CHASM SEPARATING US FROM THE MILLENNIALS.

There are three established streams of our concern about the supply chain. The first, and most acute, is that we see the supply chain itself as a source of vulnerability and risk to the operation of the critical computer systems themselves. The whispered fear is that of malware lodged deep in silicon by a powerful nation state adversary. A legion of cyber sleepers invisibly infiltrated in to every one of the computing devices upon which we know we depend. The hidden menace. Living undetectably amongst us, silently awaiting remote activation. Alien invaders capable of bringing about our total destruction.

The second is that we see the supply chain as a vector for the execution of the intention of hostile actors such as criminals and intelligence agencies. Here the recent thefts from the Port of Antwerp stand as the exemplar. The third is the damage sustained if the supply chain itself ceased to operate and the supply of computing technology was threatened.

In addition, there is now an emerging stream of concern about the vulnerability of the supply chain to infiltration by counterfeits and forgeries of the products of established and trusted brands. This will mature rapidly to reciprocate and magnify the first and foremost of our concerns.

Our anxiety is amplifying, edging us closer to a 'something must be done' response to a sense of impending crisis. We must now pause and ask

ourselves this; to what extent is this sense of crisis borne out by evidence and analysis? Or, from a different direction; to what extent is our sense of crisis the result of a panic reaction to a new context that we neither understand nor control? To what extent are we victims of future shock? Are we holding ourselves prisoner in Cold War bunkers of the mind?

There is no doubting either the complexity of our supply chains or the fact of the existence of manifest vulnerabilities. Computers are artefacts of profound and increasing supply chain complexity. Supply chains are atomised, fragmented, volatile, unpredictable and unknowable. Key components are, and will continue to be, designed and manufactured across the globe. And so in areas where those with hostile intentions towards liberal democracy can operate with greater tolerance and latitude than would be possible in the established heartlands of these democracies. The location of assembly of the components in to a finished market-ready device is, in terms of the assurance of the supply chain, irrelevant. Assurance models predicated on the susceptibility of devices, let alone systems, to code or component level recursive analysis are, at best, redundant.

Assertions of the abstract fact of the existence of vulnerability devoid of context, data, or substantive rational argument, are as useless in generating meaningful utility as they are attractive to those with something to sell. Even in the most benign of circumstances, they are an insufficient basis for action. In times of limited resources, they can easily become the cause of costly and unproductive failures. When the subject of concern is itself a societally critical phenomenon, then the raising of defences that will inevitably reduce the beneficial effects of the thing being protected, should not be lightly undertaken. To destroy a thing in order to protect a thing is an unacceptable price to pay when we depend upon that which we defend for our very existence.

As I write this, the British Prime Minister, David Cameron, has just returned from leading a delegation of senior business leaders on a trade mission to China. He returned for the debate in Parliament on his coalition government's Autumn Statement. Whilst in China, the Prime Minister faced down criticisms that he was sacrificing a commitment to human rights, asserting that he was "unapologetic" about his emphasis on the economy. Britain, he observed, is a "trading nation"[1], and as such, whilst "some in Europe and elsewhere see the world changing and want to shut China off behind a bamboo curtain of trade barriers, Britain wants to tear those trade barriers down"[2]. During his trip, the Prime Minister pressed the Chinese authorities openly for a "proper cyber dialogue" whilst at the same time choosing to highlight that "we need … to up our investment in cyber security and cyber defence" because "there is an enormous amount[3] of work to be done". The "Global Times", a nationalist leaning tabloid owned by the Communist party, ran an editorial arguing that "the Cameron administration should acknowledge that the UK is not a big power in the eyes of the Chinese. It is just an old European country apt for travels and study"[4].

These stories encapsulate much of the difficult realities of our age. David Cameron travels to China to bid for business. China needs access to the economies of Europe and America if it is to continue to grow just as it holds the old world in aloof contempt. David Cameron returns to the UK for a debate on a bill that legislates for further austerity in order to counter the effects of a financial crisis precipitated by a failure of the US and UK banking systems. The financial crisis itself revealing that a longer

term strategic shift in the axis of geo-political and macro-economic power had been underway for many decades; masked latterly by a credit fuelled boom in consumer spending. Chinese concerns continue to invest heavily in overseas infrastructure of every sort; including the next generation of the UK's nuclear power stations and the new high speed train system. The Internet would simply not exist without equipment of Chinese manufacture.

China and the world of which it is a part are locked together in indivisible interdependency. The rise of a middle class has been both predicate and consequence of the Chinese economic miracle. The Chinese middle class enjoy less direct political and societal power, and influence than their equivalents in the liberal democratic heartlands. The key to the continued, relative, dormancy of the Chinese middle class is sustained and substantial economic growth. Affluence, a necessary palliative to the frustrations of political impotence and essential to the deflection of the middle class from the leadership of populist protests. History teaches that an alienated and disenfranchised middle class make formidable leaders of those similarly alienated and disenfranchised elsewhere across society, and that the exercise of such leadership is far more likely during periods of extended economic contraction. The political leadership of China has no rational interest in crippling or even seriously degrading the economies of the world upon which it depends for its very survival.

There is no doubt that bad things are happening and no doubt that they will continue to happen. Individuals, companies, social constructs and nations compete, using any and all means at their disposal. We need to gather more evidence than we currently possess about the nature of these bad things as they are manifest in the cyber domain. We must quantify and analyse data exfiltration rather than simply assert its, undoubted, existence. We must contextualise our analysis and root it in the reality of the world as it is, rather than the world we once knew. We must learn a far more nuanced way of thinking and a far more agile and responsive way of acting. We must relinquish the use of two dimensional categories such as 'User', and 'State', and 'Non State'. They conceal more than they reveal; expose more than they protect.

In a minute number of cases, it will be necessary to entirely internalise the cyber supply chain. To design and manufacture the silicon wafers themselves and assemble the finished computing devices under the tightest controls possible. To render every aspect of the process the subject of full disclosure and trusted hands. The costs of this, in every sense, will be astronomical; unsustainable beyond the tiny portion of the overall requirement for which they will be essential. System capability will be degraded, agility will be compromised, and any notion of a financially prudent return on investment will be laughable. Such efforts, necessary though they will be, must be confined to the absolute minimum. Any attempt to generalise such extreme remedial counter measures as a response to the great supply chain fear would represent an attempt at economic autarky. History repeatedly teaches that attempts to pursue such a strategy as anything other than a narrow and exceptional response to extreme conditions is doomed to fail, often precipitating crisis worse than that which it sought to avoid. Lessons that Kim Jong-un would do well to re-visit as he continues the practice of the Juche ideas he inherited from his father.

We must relinquish the legacy of the deterministic systems thinking that won us the Cold War and embrace, instead, the more subtle and less certain arts of the management of complex systems through the observation of effects, and the generation of perpetual feedback cycles. We must actively enable the core structures of our systems to depend upon continuous modification of their own states. At the root of our fears about the vulnerabilities of the supply chain specifically, and of cyber more generally, is the apprehension that our adversaries have proven better able to exploit the true form of cyber than we have, and even less comfortably, the darker fear that the deep cause of our failure to counter the success of our adversaries is us.

WHEREAS THE COMMERCIAL RELATIONSHIPS OF THE VERTICALLY INTEGRATED CONSTRUCTS OF THE COLD WAR PRIZED STABILITY AND LONGEVITY, THOSE OF THE INFORMATION AGE THRIVE ON VELOCITY.

The systems of the cyber domain are unimaginably complex and inextricably interconnected. Every nation, every society, every institution of the state, every individual, our entire global civilization, depends upon this new phenomenon. Thus arises a paradox deep at the heart of our primal fears about the security of the cyber supply chain. Given precisely this complexity, and interconnectedness, and existential dependence, then, if the core silicon is infected, the execution of the attack will destroy those who perpetrated the atrocity just as surely as it destroys those against whom it was aimed. Because of the atomised, fragmented and volatile nature of the modern supply chain, it is in principal possible to plant a latent attack capability at such a low level within systems that detection is indeed impossible. However, the execution of such an attack is, literally, a zero sum game. Or perhaps more accurately, an extinction level event.

The chaos of our cyber systems is a function of their complexity. Both complexity and chaos are at the heart of the transformative and empowering qualities of the cyber phenomenon. We must emerge from our deep state of shock and denial and use the very power we have come to fear. Cyber is not amenable to command and control. Rather it must be existed within; its effect observed and unceasingly managed. Cyber is a transformation in human affairs of at least equal significance to that of the Neolithic Revolution, the Reformation, the Enlightenment and the Industrial Revolution; combined. To the extent that the computer systems upon and within which cyber exists were once ours; they are no longer so. Cyber belongs to society. Cyber is society. Our job is now to enable and empower the evolution of society through the development of a safer human experience of cyber.

Victory in the Cold War was a beginning; not an end.

This article was first published in "Technovation", March 2014

[1] *Quoted in the "Financial Times", December 4th 2013, UK edition, p.3.*
[2] *Quoted in the "Financial Times", December 3rd 2013, UK edition, p.2.*
[3] *Quoted in the "Financial Times", December 4th 2013, UK edition, p.3.*
[4] *Quoted in the "Financial Times", December 4th 2013, UK edition, p.3.*

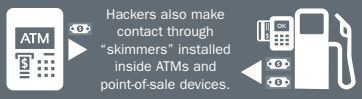
THE 4 STAGES OF A CYBER ATTACK

HOW CYBER C

ARE TARGETIN MEDIUM-SIZE

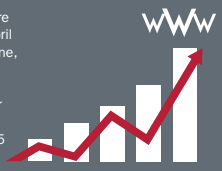
1 RISKY ENCOUNTERS

Attackers frequently make contact when an employee visits a bad website or clicks on a link in an email and unknowingly downloads malware. Wireless connections and thumb drives are other entry points.



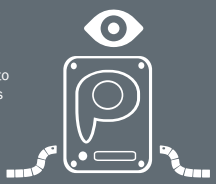
Hackers also make contact through "skimmers" installed inside ATMs and point-of-sale devices.

Criminal websites are on the rise. From April to June of 2013 alone, the number of websites "infected" with viruses or other criminal software increased 16% to 75 million.



2 BREAKING IN

Malware looks for gaps in software that hasn't been kept up to date and silently slips past users. This occurs most often on computers with incomplete security solutions.



TYPICAL SNEAKY PHISHING ATTACKS:

1. A hacker sends a consumer an email that appears to be from a reputable company. Links in the email take you to a fake website where you're asked to type in personal information.
2. You open a phishing email and a keystroke program is quietly loaded on your computer that allows hackers to later record your passwords or credit card numbers.
3. Phishers commandeer a reputable website and redirect customers to a replicated site that is used to steal customer information.

WHAT YOU CAN DO

Tell customers what information you collect and how you use it.

Only keep the sensitive data you need and delete the rest. Back up critical information.

Get the latest security software to protect your company's Web, email and devices. Find your perfect security solution at: http://www.mcafee.com/smb

Maintain operating systems, applications and Web browsers, applying patches as soon as they become available.

Allow automated updates for programs seeking to update their defenses.

Sou
McAfee Quarterly T
2013 Verizon Data Brea
Department of Homeland Security: Nati
http://www.google.ca/url?sa=t&rct=j&q=&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2Fpublications%2F
2012 National Cyber Security Asso
The Technology Policy Division of the Financial Services Ro
National Cyber Security Alliance (NCSA), http://www.staysafe
Federal Communication Commiss
http://www.bloomberg.com/news/2011-08-04/hackers-take-1
2012 National Cyber Security Associati

RIMINALS

IG SMALL AND D BUSINESSES

HACKERS TARGET BUSINESSES MORE FREQUENTLY THAN LARGE ENTERPRISES, BELIEVING YOU HAVE LESS SECURITY IN PLACE. THEY WANT TO STEAL CUSTOMER IDENTITIES, COMMIT BANK FRAUD OR FORCE YOU TO PURCHASE FAKE ANTIVIRUS SOFTWARE. UNDERSTANDING THE WAY AN ATTACK BEHAVES WILL HELP YOU STAY SAFE FROM CYBERCRIME.

3 SETTING UP SHOP

Once on your system, the bad software hides from outdated antivirus software and may even block your machines' ability to update security software.

HOW HACKERS ATTACK

Banking Trojans, malicious programs, create backdoors that allow hackers remote access to your computer and data. Cybercrooks are stealing as much as $1 billion a year from small and mid-sized bank accounts.

Malware can change browser security settings, or disable Windows Task Manager, Windows Safe Mode, System Restore, your firewall and even Microsoft Security Center.

4 DEVIOUS ACTIVITY

The bad software exports passwords, logs keystrokes, steals Social Security and credit card numbers, or snoops into your business plans or product ideas.

Your computer can even be turned into a "bot" and be used to distribute spam and malware to your customers.

CYBER ATTACKS BY THE NUMBERS

"Ransomware" locks your screen (often with a fake law enforcement message) so you can't use the computer again unless you pay the ransom. Typically, even if you pay, the hacker won't release the PC.

3/4 of attacks are driven by financial motives.

Toss anything that looks suspicious, including emails, tweets, posts and online ads.

Use a spam filter.

Protect your smart phones, tablets and gaming systems from viruses and destructive software.

Have a cyber security plan that protects sensitive information. Create Web and social media use policies for employees and make sure they follow them.

rces:

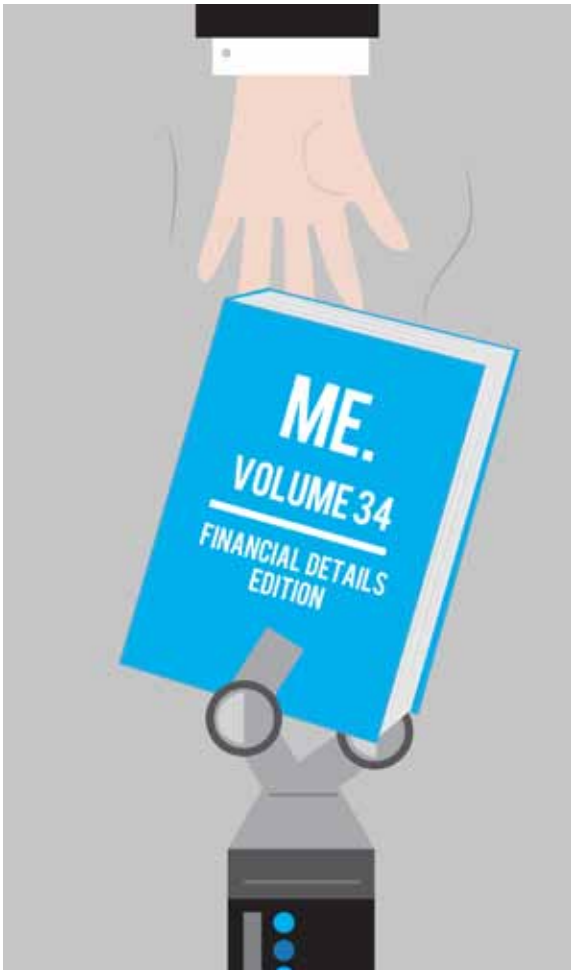
hreats Report 2013
ch Investigations Report
onal Cyber security Awareness Campaign
Small%2520Business%2520Presentation_1.pdf&ei=L7YsUpbhAeKaiQK8toDICw&usg=AFQjCNEnqKqmQJweP-J99pL4BS9I-ZpIKw&bvm=bv.51773540,d.cGE&cad=rja
ciation/McAfee Online Safety Survey
undtable, Malware Risks and Mitigation Report, www.bits.org
eonline.org/business-safe-online/resources/botnet-fact-sheet
sion Cyber Security Planning Guide
-billion-a-year-from-company-accounts-banks-won-t-indemnify.html
ion/VISA National Small Business Study

McAfee®
An Intel Company

PSYCHOLOGICAL CONSIDERATIONS OF THE

MISCONCEPTION OF ONLINE SHARING AND ASSOCIATED SECURITY RISKS

BY DR. ALISON ATTRILL, DE MONFORT UNIVERSITY



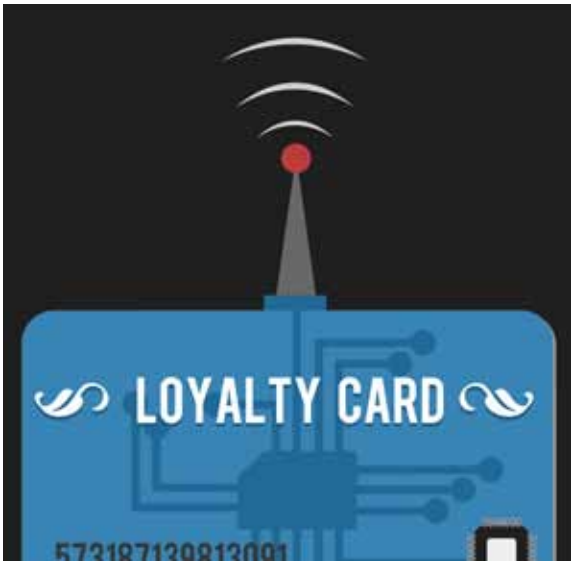
According to the mass media we all share too much information about ourselves online, making us vulnerable to security risks and threats.

Whilst the multitude and diversity of Internet arenas used nowadays, by young and old alike foster the sharing of a wide breadth and depth of information about oneself to both individual and multiple others in a single click, the notion populated by the mass media that individuals are psychologically blind to the security risks associated with that sharing is somewhat erroneous and misleading.

ONLINE SELF-DISCLOSURE

It is now virtually impossible to complete any online activity without divulging some self-information, so-called self-disclosure. From the involuntary but necessary sharing of personal details to complete financial transactions to the voluntary sharing of intimate and private details about one's daily life via social networking sites; some level of self-revelation is essential for completing almost any online activity. These activities, or behavioural goals, can be wide-ranging from online banking, information seeking, gaming, shopping and communicating via diverse mediums such as email, video conferencing and instant messaging, to socialising via social networking sites and the most fundamental of human interpersonal interactions, the seeking of a new life and/or romantic partner via Internet dating sites. All of these activities can be interrupted or manipulated by individuals who seek out such personal information with nefarious intent in mind.

If we believe the mass media, most individuals are oblivious to these risks of sharing too much self-information on the Internet and to this possible malicious intent. From a psychological perspective, this is simply not the case! To the contrary, there are some positively distinct advantages to interacting with both known and unknown others online and with pursuing diverse behavioural goals online. The Internet provides an excellent arena for the exploration of one's self-image, self-definition and self-evaluation. The psychological trade-off for these activities is the necessary sharing of self-information to attain those goals, with self-disclosure being managed through a number of psychological processes that minimise security risks. One such process is that of privacy concern.



PRIVACY

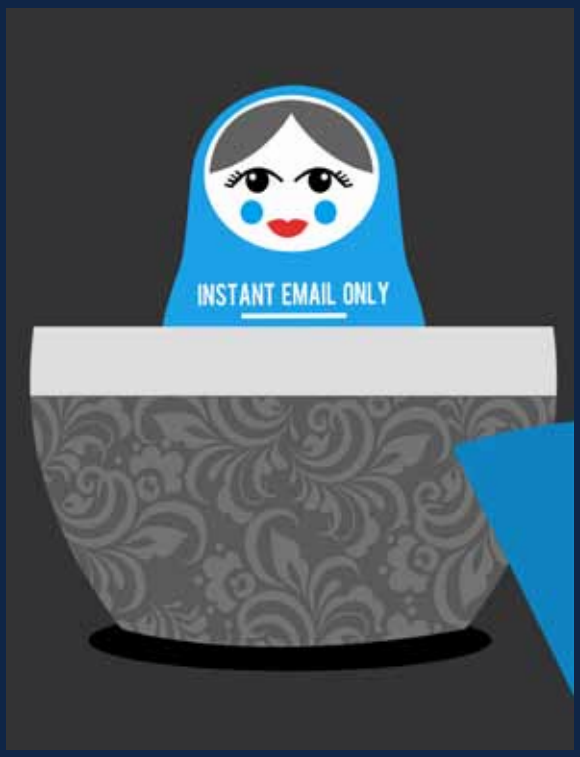
Psychologically speaking, there are a number of different types of privacy. Whereas the term privacy might mean the protection of personal data to one person, it could suggest no third party monitoring in online communications to others. Offline, peoples' privacy concerns fluctuate in relation to their need for divulging personal information to others to attain certain behavioural goals. This privacy concern is subjective and often associated with personality traits such as extraversion or dispositional trust. Our regulation of the information we share online is not overly different. Online self-disclosure is influenced by many factors to create a complex interplay of when, why, where and how people reveal personal and detailed information online. It might be the case that the influencing factors and goals of online and offline activities are guided by different processes. For instance, offline, people voluntarily forego privacy concerns in return for the rewards offered by supermarket loyalty cards, yet they would not divulge their address, telephone number and further identifying information to a checkout assistant every time they shop. Online, the same information is a prerequisite for most financial transactions, and we readily provide that information, often without reading the terms and conditions of any given website. Our only desire or goal in that moment is to complete the transaction as quickly and easily as possible. Nonetheless, we are likely more aware of the security risks associated with such single instances of online disclosures than of the risks associated with building up a catalogue of shared information across a multitude of diverse websites.

CROSS-MAPPING & DIGITAL DISCLOSURE

One of the aspects of online behaviour that is not easily replicated offline is the mapping of personal information across different types of website. It is this cross-mapping that could pose the risk which Internet users appear to ignore. Information shared on social networking sites can, for instance, be easily related to that shared on LinkedIn or ResearchGate, and even to sites such as ancestry.co.uk. This mapping could provide the basic information required to build an identity and engage in criminal activity. It is the psychological ambivalence to this possible verification of information across websites that could pose more of a security threat to Internet users than the type of over-sharing that we are regularly warned of in the mass media. Sharing across Internet sites in this way also poses another threat, namely a possible ignorance of the longevity of digital baggage. Information shared online rarely, if ever, really disappears! It may thus be this digital baggage across a multitude of websites that creates a security risk to online self-disclosure rather than simply over-sharing self-information online. Conversely, individuals might imagine themselves to be selectively sharing different types of personal information on different websites.

GOAL DIRECTED SHARING

Research is emerging to suggest that individuals are indeed seemingly selective in the material that they share on different types of website. We have been carrying out research to assess which factors most influence when, where and how people are likely to share information online in our Cyberpsychology Research Group at De Montfort University. In any form of personal communication or relationship building, it is considered the norm to initially share superficial information, with the gradual exchange of more intimate and personal material cementing a relationship over time. The length of time from this superficial sharing to revealing personal and detailed information is influenced online by a number of factors, including the type of website or application being used for an exchange, peoples' perceptions of how real and consequential their online revelations are, both to their online and their offline existences, and the level of both situational and dispositional trust that they have in both the technology used and in their communications partner(s). Another important factor is the goal-directed nature of online behaviour. People use different websites to satisfy different behavioural goals and needs. It would therefore be somewhat erroneous to treat the Internet as a homogenous arena where the same types of information are shared regardless of what people are doing and with whom they are interacting online. In line with this, our research also demonstrates that self-disclosure online is less of a splurge but more of a selective sharing process that is tailored to achieve a desired website-specific outcome. People selectively reveal self-information relating to their interests on online shopping sites, for example, but are more likely to share their intimate feelings and beliefs via instant messenger type communications than via public status updates on social networking sites. The heighted self-disclosure reported by the mass media may thus reflect the sharing of increased amounts of superficial rather than personal or intimate information.



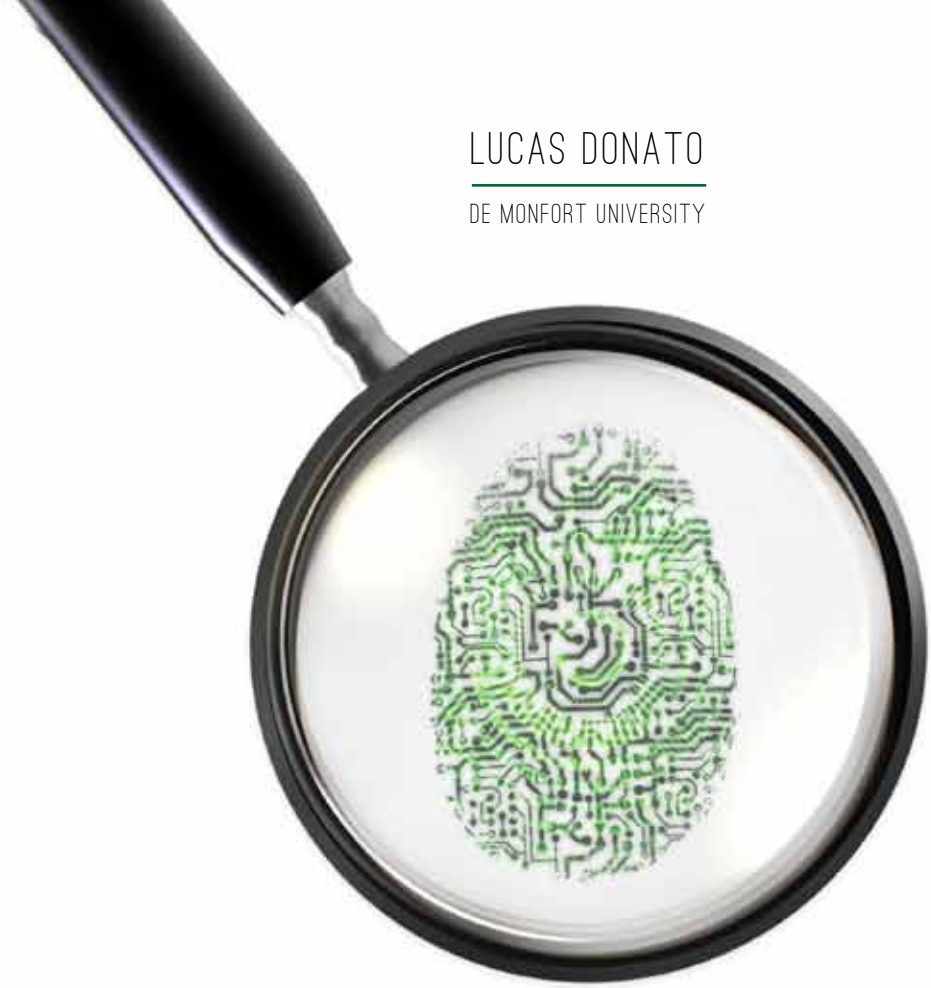
CONCLUSION

The question that arises from these brief considerations is one of the accuracy of the mass media portrayal of oversharing self-information online. It would appear that the over-sharing of personal information on one specific type of Internet site is not the source of security risks. Rather, a combination of the build-up of information across different types of Internet site, digital baggage and psychological ignorance of the cross-mapping and verification of that information, even under the guise of selective self-disclosures, could be the source of security risks to online activities.

DR ALISON ATTRILL IS A SENIOR LECTURER who leads the Cyberpsychology Research Group at De Montfort University. Her research spans a wide range of Internet behaviours, focusing on online relationships and sharing self-information online. She is particularly interested in perceptions of trust, privacy and security risks associated with online sharing.

LUCAS DONATO

DE MONFORT UNIVERSITY



PROFILING

CYBER OFFENDERS

Finding its roots since time immemorial, criminal activity has always been part of a cat-and-mouse game with Justice.

In the last decades, we have seen this game gradually transposed to the cyber domain as well, where crime discovered a new and broad field for its perpetration. Never was it so easy to find a new victim or a group of victims – they are in reach of a criminal's fingers – and never was it so easy for criminals to hide their whereabouts and identities.

Though in this cat-and-mouse game our investigative techniques and tools have evolved with time, so have the modus operandi of cyber criminals. We need to admit that we are facing some interesting challenges. No, we are not talking about the classic *"It wasn't me, it was a Trojan in my computer!"* argument. We are talking about a wealth of hiding mechanisms like anonymous proxies, compromised computers, public internet cafes (virtually, we have internet access everywhere!) and anonymity networks like Tor, i2p and Freenet, all of them being misused and making life harder for law enforcement. Criminals are enjoying all these means with a unique sense of freedom and impunity to promote a black market and sell drugs, guns, criminal services, organ trafficking and share child pornography.

Actually, these mechanisms are being used by a broader group, classified as "cyber offenders" in this article and related literature. This group of individuals includes not only typical cyber criminals, but also state-sponsored actors who engage in attacks against foreign critical infrastructures as well hacktivists spreading their word and launching DDoS attacks against their target of choice. It does not matter which class of individual we are dealing with. When we need to figure out who is behind that masked IP address in our log files or who is behind that fake Twitter account, the "attribution problem" rises.

While dealing with such a challenge, maybe we should think whether we are overlooking all those roots of criminal activity – offender activity here - and how they usually can be manifested in a crime scene. The cyber offender is clearly enjoying some advantages, so we need to adapt ourselves. As said by Collin Williams in the welcome message of this magazine's first issue, *"we must re-think our approach to the pursuit of the safety and security of the human experience in the cyber domain."* It makes sense here.

A digital crime scene is still a crime scene, and a digital crime (or digital offence, in broad terms) is still an act that has at least a minimum of planning, counts on at least a minimum of resources and it is committed by an individual or a group of individuals with specific motivations. We should agree that most methods and tools are new on cybercrimes, but when we are talking about revenge, activism,

challenge, profit… hmm… these motivations don't seem to be so new… they are inherent to the human being. Risk appetite, attack inhibitors? They are too. Since technology is therefore just a means to commit a crime, we should revisit some useful approaches to dealing with traditional crimes and analyse whether they could be of help while dealing with cybercrimes as well. When all types of crimes or offensives share some features – like human motivations, human traits expressed through behaviour evidence in a crime scene, signature aspects (just to name a few) – we should mention for sure the scientific discipline of Criminal Profiling. The study of the criminal behaviour and its manifestation in a crime scene has been explored for more than a century by the discipline, which infers a set of traits of the perpetrator or group of perpetrators of a crime by the examination of the criminal evidence available.

This set of traits - a "profile" - can be elaborated containing features like skills, resources available, knowledge, motivations, whereabouts and so on, depending on the evidence available and depending on which conclusions we could reach about them. Then, this profile becomes a valuable additional tool to assist investigations – with at least a 77% rate of success according to a research done in the 90's (Theodore H. Blau). With these encouraging numbers, and knowing that cybercrimes share some roots with traditional crimes, the idea is to apply the same concepts to digital investigations. According to the literature, the main objectives that can be achieved by applying profiling on investigations are:

- Narrowing down the number of suspects.
- Linking cases that seem to be distinct.
- Helping define strategies of interrogation.
- Optimising investigative resources (e.g., "let's focus on where we have more chances to find evidence").
- Help develop investigative leads to unsolved cases.

Actually, advantages are not restricted to digital investigations. When we have a profile of a cyber offender in hand, we are able to develop better countermeasures against their attacks. This is especially important when we are dealing with advanced offenders, like APT.

The good news, when we talk about how broad the options are for cyber offenders to hide themselves behind computer attacks, is that profiling can be a broad tool as well. Recalling the Locard Exchange Principle, the offender always leaves traces in the crime scene. And some of them can be of behavioural nature. Depending on the level of interaction an attacker has in a digital offence (e.g. a manual attack vs. an automated attack – or a single web defacement VS an attack that involves a huge team of skilled offenders and many interactions with the target), we could have different levels of traces left on log files, network traffic, social networks, chat networks, file systems of compromised machines, e-mail messages, defaced websites, instant messaging.

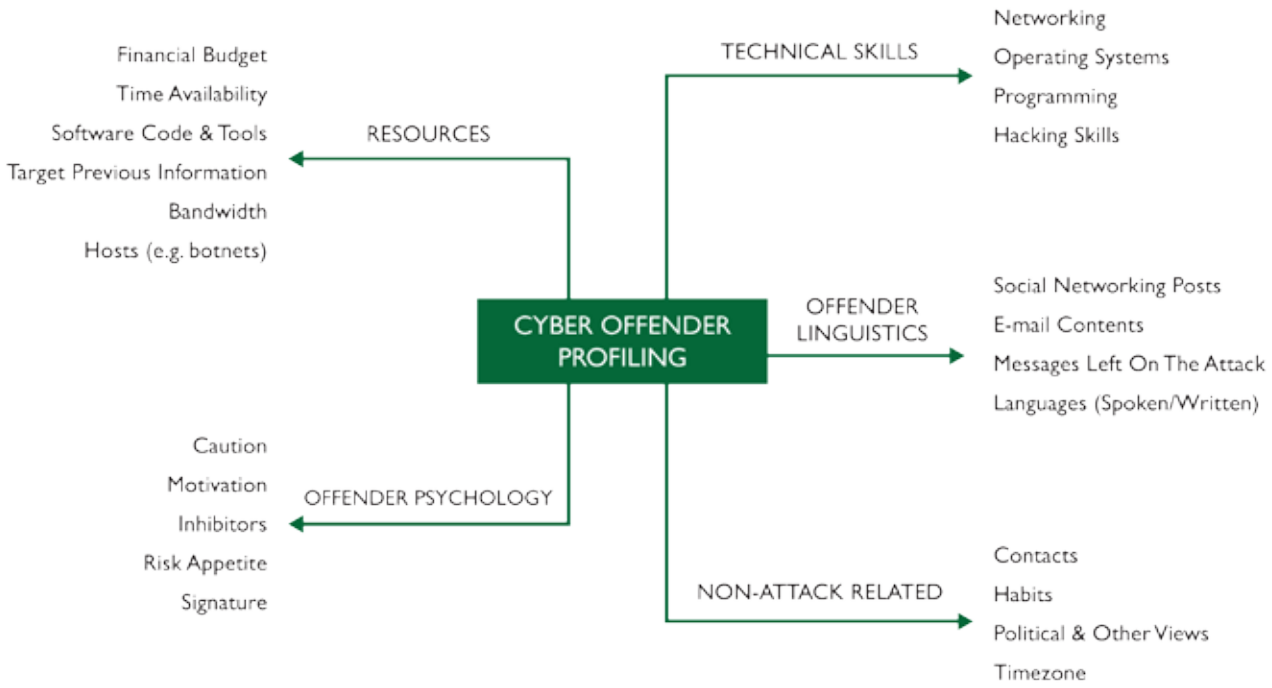
Therefore the mindmap featured below is just a non-exhaustive set of features that we can explore and work on.

Going deep, the following list is a very small set of examples that we can search for during the investigation to help populate our mindmap:

- Analysing the time between probes in a port scanning.
- Identifying motivation [revenge, curiosity, challenge, profit, to be part of a group, usage of computer resources, platform to launch other attacks, dispute between individuals or hacking groups, profit, cyber terror, hacktivism, cyber warfare, etc.]
- Analysing victimology.
- Performing authorship analysis on spear phishing e-mail content, social network posts or on software source code (looking for patterns, errors, preferred programming functions, sophistication, etc.)
- Identifying the type of tools employed during an attack and evaluating their availability (public? commercial? restricted?), required knowledge to operate (Tom Parker has conducted very good research on this topic.)
- Analysing offender activities on social networks, ranging from their first followers/following, closest contacts, word frequency, periods of the day in which activities are more intense, evidence of planning actions, etc.
- Analysing global or regional political/social/religious/economical events that could influence in the commission of the offensive.

The topic is vast and encouraging, and we can go much further. But the final message here is: we know that there are a multitude of means and technologies that are being (and will be) used by offenders on the perpetuation of their actions. But we need to know that there is a multitude of means to catch them as well.

Lucas Donato, CISSP, CRISC, is an information security consultant who currently works at a Brazilian bank. In the last ten years he has been involved with penetration testing, vulnerability assessments, incident response and digital investigations for some of the biggest Brazilian companies. Nowadays, he is pursuing his PhD degree at the Cyber Security Centre of De Montfort University, exploring the ins and outs of criminal profiling applied to digital investigations.



vmware

SBL

Cloud can be confusing. Your cloud doesn't have to be.

When it comes to cloud computing, everyone seems to have a different point-of-view. It can be pretty overwhelming. Together with VMware, the global leader in virtualization and cloud infrastructure, we would like to help. We're here to cover the important topics, provide the latest research and answer all your questions. And when you're ready, we'll help you build the perfect cloud solution, one that leverages your existing IT resources and aligns seamlessly with the specific needs of your enterprise. So, ask away and let's get started with your cloud.

Get your questions answered at www.softbox.co.uk/ourpartners/vmware

SILICON ROAD

Scott Cattaneo, SBL

"No one would have believed that in the last years of the 19th century that human affairs were being watched from the timeless worlds of space.

No one could have dreamed we were being scrutinised as someone with a microscope studies creatures that swarm and multiply in a drop of water.

Few men even considered the possibility of life on other planets. And yet, across the gulf of space minds immeasurably superior to ours regarded this Earth with envious eyes and slowly and surely they drew their plans against us."

You may recognise this as Richard Burton's introduction to Jeff Wayne's adaptation of "*The War of the Worlds*", however if you change the century, change the reference of Earth to the west, replace the antagonists of the story from Martians to the Chinese, it starts to sound like a series of messages I've heard repeated in Information Assurance and Cyber Security forums, events, and symposiums over the last 2 or 3 years.

Or specifically; components that originate in the Far East are intentionally contaminated and sent through the supply chain ready to wreak havoc upon their designated end-points, or to lay poised for some coordinated attack against western interests.

Repeat such theories in the voice of Marvin the paranoid android from Douglas Adams' legendary "*Hitchhikers Guide to the Galaxy*", and you start to establish

components that originate in the Far East are
intentionally contaminated and
sent through the supply chain
ready to wreak havoc

the correct IA Conference tone, i.e. plenty of doom and gloom with no answers or even suggestions offered about what we should actually do about it.

"I can calculate your chance of survival, but you won't like it". Okay, enough flippancy. This article is not designed to offer opinion in respect to the validity or credibility of such paranoia (if it is indeed paranoia). The point of this article is to provoke debate about solutions to this potential dilemma, in the hope that we can move this stalled and stagnant area of discussion forward to another stage.

To explore the issue I'd like to begin by describing an idea that we had recently. This idea was to provide inter alia, some upstream supply chain information that could potentially assist our customers. It involved the creation of labels similar to the type that provide nutritional information on food packaging, but for the IT products that we sell to our customers. These would become "Supply chain safety labels" chiefly designed for those within the government and national infrastructure markets.

Within our due diligence and product on-boarding process used to bring on-line new additions to the portfolio, we ask for, and record the following information about the products put forward for adoption:

- Country of origin
- Countries where the R&D and assembly occurs
- Location(s) of major financial stake holdings and subsidiaries
- Plan(s) in respect to on-going support arrangements for the intellectual property (e.g. Source code)

All these questions are designed in some way to protect ourselves and our customers from risks inherent in a global supply chain, as well as within the rapidly developing and volatile IT industry.

The idea then developed a secondary element whereby we would list this information on quotes in the form of a "Traffic Light Scheme" to assist customers in identifying supply chain risks. We never did get around to finalising the criteria for such a labelling scheme, but for the point of illustration it could have read:

GREEN = wholly "five eyes" supply chain – Assured Supply Chain
AMBER = supply chain within the NATO member nations
RED = global supply chain – Unassured Supply Chain

Playing devil's advocate on the development of the Traffic Light Scheme, we soon realised we could get ourselves into trouble undertaking such politically sensitive discriminations without some serious governmental backing to which we could refer. Based upon this fear we decided to stick to plain labels only.

But I then asked myself "But who really cares?" as in REALLY cares?

If I quoted 2 options (1 green & 1 red), and the red was 10% cheaper than the green, who would really consider paying more for the "Assured supply chain" option? Are we paranoid to the degree that we apportion a tangible risk factor, which then translates to an economic buying decision based upon the value of a weighted risk?

I am yet to witness any formal discrimination with respect to location of the origin or assembly of technology made by our customers.

A global supply chain is extremely complex, and the context in which it is perceived changes dependent upon your own location and associated risk factors. For instance, IT has distinctly different supply chain structures for Software, Hardware, Services, and Cloud Services.

Taking Cloud Services as an example, in particular referencing the G-Cloud framework prevalent within the UK public sector, effort has been exercised to actually address supply chain assurance issues.

Due to the very nature of Cloud Services in that they transmit and host sensitive data, threats of compromise appear to be more direct and immediate. To address these threats, G-Cloud introduces the concept of an accredited "UK Safe Harbour"; UK only domains perfect for SME's to engage in. This in turn serves a separate government agenda regarding the wider utilisation of SME's in the public sector supply chain.

It is widely recognised that larger global vendors who have based their data centre operations almost exclusively in geographic locations that are more economically viable and therefore not within the UK, have held back the adoption of Cloud Services on a large scale, and specifically within the public sector. This is especially true when it involves departments outsourcing the more critical or sensitive elements of their business processes to an external third party.

Dependent upon who you are and/or what you do, encouragement through policy and potentially mandate could direct departments to only accredited service options, where for example, the data transfer and hosting remains within a trusted UK domain.

Therefore is the threat of data theft through unauthorised access via a compromised data centre greater than the threat of data loss/leakage through an exfiltration hack initiated through intentional corruption built into the software or hardware? We certainly worry about the former sufficiently to act upon it (e.g. G-Cloud – UK Safe Harbour), so why not the latter? Is it just too hard, expensive, or overwhelming to begin to think about? Or do we simply worry less?

Maybe we should worry less. After all, infiltrating a highly mechanised and automated factory production process would contaminate a huge quantity of devices shipped to many separate locations all over the world. This type of attack would surely be out of reach of the criminal fraternity, whereby their intent and subsequent targets would be far too defined and specific to attack effectively in this way. Threats of these attacks would therefore be restricted to state sponsored objectives, and can then be, to an extent, predicted by current global and political intelligence.

Even with state sponsored attacks, infiltrating an outsourced design process or a semi-conductor foundry for example, would be very difficult and expensive. Plus, the further upstream in the supply chain you infiltrate, the more difficult it would become to home in on any specific targets.

Nevertheless if we conclude the threat to be real, could we create a similar set of circumstances for the analogue and corporeal supply chain as we do that of the digital in respect to the G-Cloud model? I acknowledge this would be extremely difficult and the costs would be eye-watering, but if we really worry about the threats of adopting a global supply chain (after all, over 50% of chip production revenue originates in China), then is this worth considering? At the very least, is this worth considering for specific acquisitions made by our High Threat Club for instance?

It has already been done to an extent in the US. The NSA has initiated the Trusted Foundry Programme, creating an assured supply chain including 50 accredited suppliers for DOD or DOD-sponsored critical requirements.

This addresses some of the issues, at least with production vulnerabilities (though not chip design vulnerabilities) but it is expensive and restricted to only the most critical defence requirements. The vast majority of Federal and Infrastructure capability remains at the mercy of the global supply chain, and for economic reasons alone, will no doubt continue to be so for the foreseeable future.

Could it be feasible to create a quarantine process that specific high threat customers could use? This would be a cyber-equivalent of how we treat the movement of animals across continents. These quarantine areas could use technology currently available, or develop new capabilities that conduct deep inspection activities testing for intentional hardware and software corruption, or use techniques to prematurely trigger payloads that contaminated products may host. This would clearly delay shipments, however if we believe the threat to be real then is it worth investing in this type of quarantine system or clearing house for IT imports?

In summary we need to ask ourselves, and at least attempt to answer a series of questions, notably:

- Do we believe that state sponsored threats of this nature actually exist within the supply chain?
- Do we have any evidence that they do?
- If not, what are we doing to the gather that evidence?
- What can we actually do to mitigate any risks based upon any evidence we collect?
- How does each layer of our public and private sector markets evaluate these threats as risks (assuming that through the collection of evidence we have determined that they do exist)?
- How then, do these risk weightings translate to economically sensitive buying decisions?
- Based upon this economic translation, what realistic options remain open to us? i.e. what should we be doing to mitigate and reduce the risks of supply chain contamination?

A global supply chain is extremely complex, and the context in which it is perceived changes dependent upon your own location and associated risk factors.

Using a process of trigonometry the answers to these questions could for instance, equate to:

- Exercise a programme of activity to diplomatically engage potentially antagonistic nations on these subjects, whilst attempting to gather evidence that supply chain threats exist.
- Invest in / subsidise the creation of an assured supply chain. This could also constitute an emergency supply chain for our critical functions. This would in turn mitigate threats to availability, e.g. in the wake of major natural disasters like the recent floods in Thailand.
- Develop quarantine areas. Technological challenges will have to be overcome; however this activity could for instance be outsourced to trusted, specialist, and local SME's who could usefully take up some of the burden.
- Based upon lack of evidence or confidence in state sponsored intent, accept and acknowledge a residual risk of supply chain contamination, and move onto to the next problem.

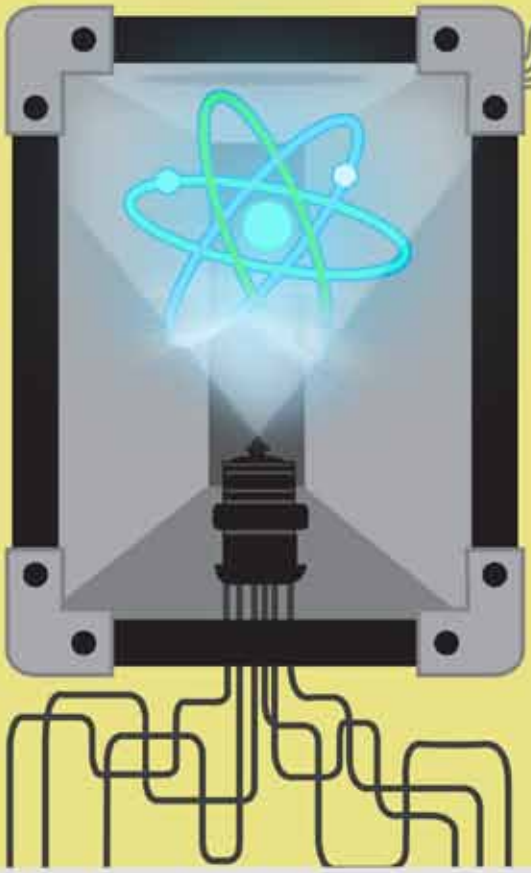
Any and all of these options are difficult, complex, political, dynamic, and localised all at the same time, and it's certainly not an exhaustive list but we do need to do something other than continuing to proffer doom. We need to break the inertia that this attitude has developed. There is just no value or utility in rehearsing the problem space, and continuing to perpetuate fear, uncertainly and doubt.

Despite depositing this notion of paranoia I acknowledge that a threat must exist, but what is the actual risk? And whilst I can agree that the problems will persist, and in many respects we face insurmountable challenges in regard to the complete safety of a global supply chain, there must be immediate opportunities to improve the situation and at least mitigate and reduce the risks of supply chain contamination as things now stand.

But what is the level of motivation? What will move us beyond talk and into action? Are we waiting for a compelling event? Or are we prepared to implement some mitigation strategies now?

To conclude, I would be extremely interested in your feedback on these issues. In particular, do you think the "Supply chain safety label" idea described earlier actually has value? Your voice literally determines the action that we take in respect to developing this system, as in the spirit of this article we will endeavour to play a positive role in moving the debate forward if this idea is deemed to have genuine utility.

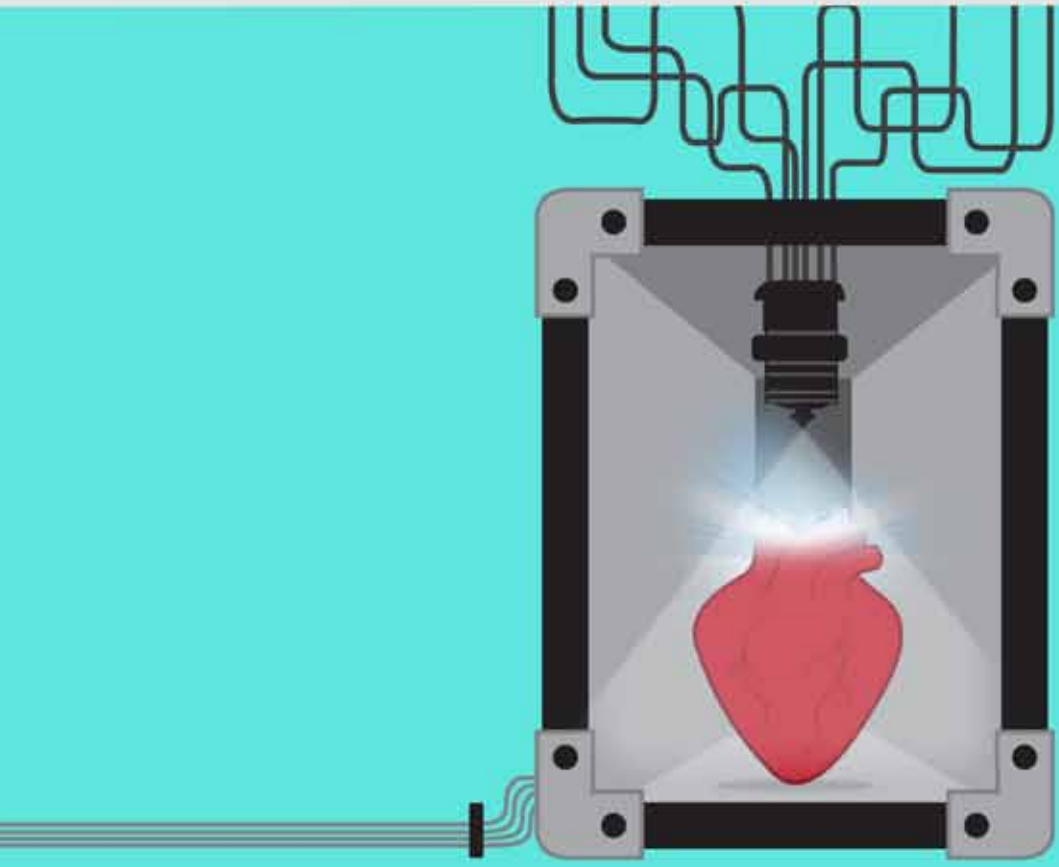
P.S. In researching the concept of paranoia for this article I called the National Paranoia Society. The person who answered wondered how I got his number…..(sorry).



FROM 3D PRINTERS TO 'NANOFACTORIES':

A BRANCH OF TECHNOLOGY WITH REVOLUTIONARY POTENTIAL

BY TOM HOOK, SBL



3D printers are becoming more and more widely used, with the inherent technology being developed persistently and rapidly.

These devices already have practical purposes, even with their use still in its early stages. How conceivable is it that the technological capacity of 3D printers will increase to the atomic level, with their owners able to build literally anything (including food)? It's practically a certainty, according to those at the forefront of nanotechnology. What's more, these 'nanofactories' will be in every home, affordable for everyone, making each household completely self-sufficient and turning modern society on its head.

Nanotechnologies are already able to achieve astounding feats. Lockheed Martin, for example, have developed a membrane just one atom thick, which can be used to desalinise and purify sea water, potentially solving the global drought problem. Nanotechnology's potential is also being steadily unlocked for use in pharmaceuticals, and the World Health Organisation (WHO) has said it vastly increases the effectiveness of drugs in the fight against superbugs, and their growing resistance to antibiotics.

The commercial prospects of 3D printing are also progressing rapidly. Asda, for example, have recently toured the UK offering a 3D scanning and printing service, allowing customers to make a model-sized ceramic replica of themselves. Websites are also cropping up which now operate almost in an Amazon style, where customers can browse objects, such as mobile phone cases and, instead of having the item delivered, can instantly download the 3D design and print it on their household 3D printer.

Combining 3D printing principles with more complex technology is already being explored, as bioengineers are now using living cells in the printing of functional liver segments. With the ability to 3D-print whole, functioning organs seemingly not too far away, it's clear that the commercial potential of this technology will expand far beyond building your own mobile phone case.

The possibilities, according to Broadcaster and Technology Commentator James Burke, are limitless. He recently predicted that in 40 years, everyone will have their own nanofactory (an atomic-level 3D printer), and we will be able to produce anything we could ever want, including food, for free. This, he explains, is because the ingredients soil and water atomically provide everything needed to build any physical object (provided you have electricity and some acetylene gas). Houmous, a t-shirt, crockery; anything you want, this technology can create from almost nothing – a concept identical to *"Star Trek's"* on-board Replicator, but this time non-fiction.

The ability to personally produce our own goods, according to Burke, will abolish the need for money, as the population will be totally self-sufficient. If people no longer need money to make purchases, they won't have to work in order to earn money. This would bring about total economic collapse and, Burke argues, the abolition of government (as the main purpose of the state is to ensure appropriate redistribution of wealth, which will no longer be needed).

Burke's claims also include the gradual disappearance of cities, as the only need for people to live in large collectives now is to be near their place of work, or source of food (i.e. shops). He says that people can choose to live self-sufficiently anywhere they want (including in the most idyllic and remote locations in the world), and will most likely spread out to live as individuals, or in simplistic medieval-style communes, as opposed to built-up cities.

Overall, the most important change is that resources will no longer be scarce, as the world will literally be able to create as much 'stuff' as it desires. Perhaps the most vital result will be that the problems of the one in eight people in the world currently suffering chronic undernourishment, will disappear.

The time and cost it will take to get the technology to this point, however, will be enormous, and the only way that traditional food sourcing and manufacturing techniques will be abandoned is if they are more expensive than nano-production. It's impossible to say if enough funding will be focussed on making this happen. What is clear is that technology companies can't invest in this without the prospect of financial return at the other end. This means that nanofactory equipment will be prohibitively expensive to customers. On top of this, there will be a need for the design of complex software and atomic-level 'blueprints' for the catalogue of physical objects that customers will produce.

Because of the gradual development of the technology, and the costs this brings to developers, customers will need to be charged for using these devices. The scientists designing these complex product blueprints won't work for free, so to pay for their efforts, developers will most likely need to charge customers in order to download the designs to their nanofactories. Whether this charge will be one-off for the design (and then unlimited printing), or for every single print of the design, depends on the company. With the extensive development cost and infinitely higher earning potential, it's likely to be the latter. So every time a customer wants to print, say, an apple, they'll have to pay.

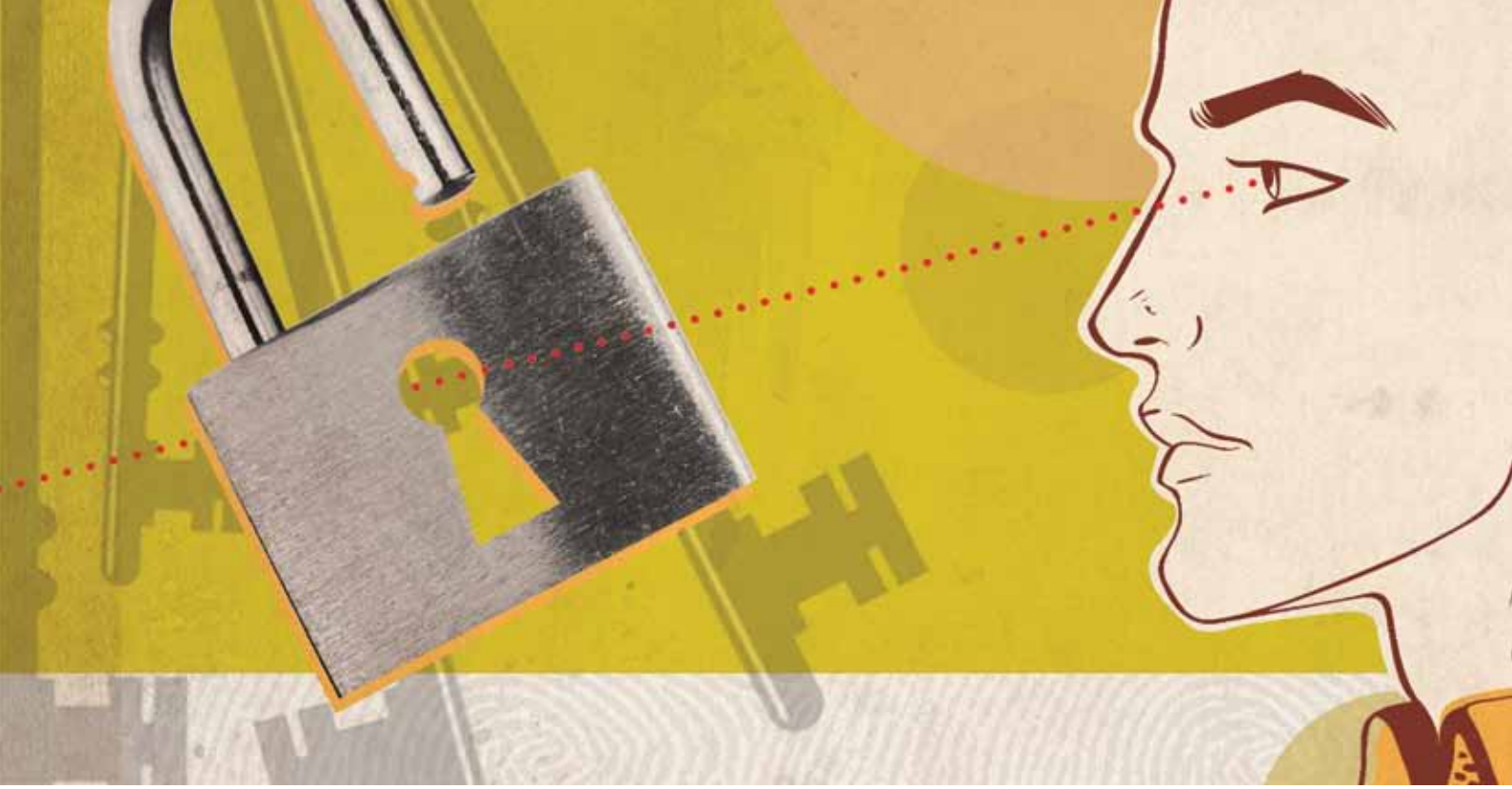
Once this charging model becomes the norm (which isn't too far away from the current websites where customers buy and download mobile phone case designs), it's hard to see how it could suddenly change and become free to use. The need for money would therefore always be with us, it will just be used in a different way. In effect, we'll all have vending machines in our homes, capable of dispensing anything we like.

Of course, with the fierce competition to provide customers with this service, it's possible that companies will find a way to offer lower and lower prices. A 'free' option may even emerge, similar to Linux, with open source software and the molecular blueprints becoming widely available for nothing; all you need to buy is the hardware. This would be a game-changer, and Burke's vision of a totally self-sufficient life seems more likely, without the need for money.

> ...'NANOFACTORIES' WILL BE IN EVERY HOME, AFFORDABLE FOR EVERYONE, MAKING EACH HOUSEHOLD COMPLETELY SELF-SUFFICIENT AND TURNING MODERN SOCIETY ON ITS HEAD..

Whichever way this plays out, it's clear the technology will change society in some way. Whether we have to pay for the things we print with our nanofactories or not, the delivery of products could easily transform to being electronic, rather than physical. The same thing that happened to music (i.e. the transition from vinyl or CD purchase, to downloads), could therefore happen to every other physical thing that we could imagine wanting.

It's impossible to know how the world will develop in light of this technology, but it is likely to transform into something unrecognisable to us, particularly with the near disappearance of the manufacturing and retail industry. These areas would come under the umbrella of 'IT', as a wealth of IT products and services will be needed to support the nanofactory's function. The IT industry would therefore grow exponentially and will be relied upon for the delivery of food and supplies. The world of IT has always explored and realised astounding achievements in the past, but with the possibility of solving world hunger and allowing the public to be entirely self-sufficient, it could be the cause of an unprecedented period of transition.



BIOMETRICS: READY FOR PRIME TIME?

MARTIN BATEMAN
UNIVERSITY OF CENTRAL LANCASHIRE

Biometric based authentication systems are being widely deployed and used. Their usage has grown to the point where governments have deployed facial recognition systems at airports to aid with passport control and off the shelf fingerprint recognition systems are available for securing anything from a laptop, a phone or a door.

The attractiveness of using biometrics is obvious, it allows a person to be authenticated without the need for them to remember yet another username and password. With a username and password it is possible to give someone your credentials whereas with biometrics it is much more difficult to transfer your credentials.

It is important to understand that the biometric authentication process is typically not a straight forward 'match' or 'doesn't match'. In the case of a username and password the authentication system is presented with a password for a specific user. If the password is a copy of the stored password then the user is authenticated to use the system. Biometric identification systems use a fuzzier process in order to perform their matching. Typically a series of features are used and matched against a stored copy of those features. Matching those features 100% would be impractical as changes in lighting, finger position or just being tired could have an impact of those features. Instead we attempt to get a close match and use a threshold as a cut off to say if the presented credentials match the stored credentials. Ideally this gives us a 'true positive' where a subject is correctly identified and a 'true negative' where the subject correctly doesn't match but we also get 'false negatives' where a subject is wrongly not identified and 'false positives' where a subject is wrongly identified as someone else. How the features are measured and compared has a massive impact on how the system classifies the subjects. In many cases we are able to tune the sensitivity of the matching but if we are too sensitive then we increase the number of false negatives, and if we reduce the sensitivity then we increase the number of false positives.

		REAL: MATCH	REAL: NO MATCH
SYSTEM	MATCH	TRUE POSITIVE	FALSE POSITIVE
SYSTEM	NO MATCH	FALSE NEGATIVE	TRUE NEGATIVE

Figure 1: Biometric matches. System is the result from the biometric system. Real is if it is an actual match.

FAILURES IN BIOMETRICS

Passport control - Facial recognition

The most visible use of facial recognition in the UK is at passport control. It allows people with biometric enabled passports to skip the manual process of having a border agent check your passport and instead it uses facial recognition to verify that the person presenting the passport is in fact the valid holder of that passport. In 2008 the system allowed a husband and wife to accidentally switch passports and were able to pass through the automatic system[1]. Ian Donald, technical director for smart card company Regis Controls stated to a Joint Select Committee that the biometrics in passports have a 10% failure rate. A GAO report on the challenges of implementing biometric border security states there is a 15% error rate for facial recognition systems as the person ages. As the holders of the biometric passports age then there will likely be an increase in failures.

[1]Luckily there was a border agent on hand who noticed the mix up.

iPhone 5S - Fingerprint recognition

In September 2013 Apple released the iPhone 5S which included an integrated fingerprint recognition system. Although it was not the first, it is, at the time of writing the most recent. Shortly after the introduction of the iPhone 5S, the complaints concerning the failure of the fingerprint recognition to recognise the user of the phone, began to appear. At the time of writing, reports are that around 20% of users are receiving false negatives when using the fingerprint recognition system of the iPhone 5S.

The use of automatic fingerprint recognition systems comes with multiple problems. Around 12% of the population have fingerprints that cannot be easily read and a NIST report states that 2% of fingerprints are impossible to read using existing technology. They could be too old or be engaged in manual labour so the fingerprints have worn off. Women are also known to have fainter fingerprint ridges than men and the fingerprint ridges in the Asian population are also faint. So it could be partiularly difficult to read the fingerprint ridges of an elderly Asian woman. Fingerprints have been known to change drastically in a short period of time due to wear from manual labour or damage such as cuts and burns.

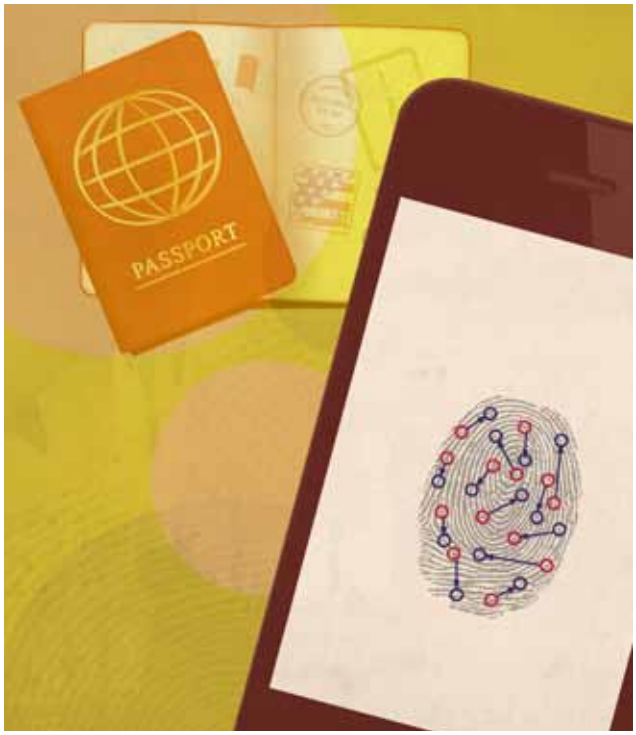
WHAT CAN WE DO?

The success of any biometrics systems hinges on multiple factors.

1. DATA COLLECTION METHOD
2. DATA SUMMARISATION ALGORITHM
3. DATA COMPARISON ALGORITHM

The data collection should be done in as consistent a way as possible. This means that the same data collection conditions should be maintained. In the case of the facial recognition system then, the lighting should be consistent, the subject should be a consistent distance from the camera so that the face is a consistent size and the subject should look in a consistent direction - straight into the camera, ideally.

The data summarisation method should be picked in conjunction with the data collection method - there is no point in attempting to use a feature that you haven't been able to record and the comparison algorithm - there is no point comparing features that you haven't extracted.



Finally the comparison algorithm needs to be as robust as possible in order to make up for faults in the data collection and extraction phases. The robustness that is needed by the comparison algorithm takes two forms. Firstly for a positive match it should allow a wider variation of features and secondly, in the case of a true negative, it shouldn't match. These two goals are in opposition, as we are more permissive with true positives then the likelihood of a false positive increases.

In order to maximise the distance between the true positive and true negative we perform a testing and calibration phase. It is at this stage that a large number of mistakes can be and are made when calibrating the comparison algorithm. The calibration process generally consists of testing the method with a representative sample of the population that will use the biometric system. The members of that chosen test sample have a large impact on the final design of the system as they provide the data that is used to calibrate it. In an ideal world, you would choose a sample set of people that perfectly represents the entire human population. In reality, that is incredibly hard to do. Finding representatives for common groups of people is fairly easy, for example finding males aged 18-40, but the difficultly comes when looking for representatives for minorities, and as the minority represents less and less of the general population then finding representatives to make up part of the sample becomes increasingly more difficult.

As the minorities are either under-represented or missing from the training sample then any physical variation will not be part of the training, and is therefore unlikely to be accounted for in the final system.

So what can we do to increase the success of biometric systems? The use of representative samples of people when testing biometric systems will greatly help in their accuracy and will allow for a larger coverage of the population when using biometric systems. Combining multiple biometric systems, or by giving people the choice of which systems to use. Regularly updating the biometric database will allow for changes in the person as they age. In the short term we cannot rely on biometric systems to be 100% accurate, there will always be variation within the population and until that variation is taken into account at the very start of the design of the biometric system then there will always be failures.

Hasta la Victoria, Folks!

WHY ANONYMOUS SHOULD UNMASK NOW
OR RISK BECOMING CAR SALESMEN

BY ANDREW COOK, SBL

On 31st January 1606, a battered and beaten Guy Fawkes walked to the gallows in front of a baying crowd of thousands. Amongst them was the very man he was charged with attempting to assassinate – King James I of England.

Fawkes had been drawn from his prison in the Tower of London to what would be his final destination, Old Palace Yard, Westminster. Here he was due to be hanged then have his body quartered and sent to the furthest reaches of the realm. Choosing to throw himself from the scaffold and break his own neck rather than face any further torture, Fawkes' lifeless body was nonetheless mutilated and dismembered as a warning to other would-be traitors.

Skip forward 350 years or so to 9th October 1967. In a Bolivian schoolhouse, Ernesto "Che" Guevara was shot 9 times through the neck, arms and legs in a military execution designed to give the impression that the Cuban revolutionary had been killed in action. Guevara had been captured two days earlier by Bolivian troops and CIA operatives, interrogated and then killed before his supporters had chance to retaliate. In the years preceding his capture, Guevara had fought to forcibly remove large American corporations from his adopted Cuba and helped to spread Marxist ideology throughout Latin America and the rest of the globe.

These men's deaths were not as simple as an eye for an eye. Fawkes died not purely because he tried to kill the King but because he fought to upset the status quo. By attempting to remove the Protestant monarch and begin a Catholic rebellion, he and his twelve fellow conspirators made challenge to the very foundations of 17th century Britain and for this it was deemed he could not be allowed to survive and must be made an example of. In the same way Guevara's death was not ordered because companies such as the United Fruit Corporation were no longer allowed to trade in Cuba, but because of the ideas he embodied. His growing world standing and outward appearance as a genuine ambassador for Communist ideals offered too much of a threat to his predominantly capitalist neighbours.

The comparison between the two runs deeper. Both were relatively well educated, brought up in respectable middle class families, yet motivated to strive for immense social change. Neither was a stranger to war and conflict and both were, by all accounts, talented and passionate orators. Today the faces of both still resonate as a symbol of resistance to fascist regimes, overbearing government repression and corporate greed.

That's the romantic version anyway. The problem is … they don't. Regardless of whether you agree with their politics or methods, both men can be admired for taking a stand for their beliefs. Whilst many stay at home in silent disagreement, these men willingly gave their lives for what they believed to be the greater good. Today though, they are no longer seen as human beings who lived and breathed and walked upon the earth. Their legend has become such that they are now no more real than the likes of King Arthur or Robin Hood.

> **"The inconvenient truth is that Anonymous' rise in notoriety owes more to its PR machine than its ideology."**

Che Guevara's longevity as a cultural icon is entirely thanks to the very economic system he sought to destroy. Today his portrait "Guerrillero Heroica", taken by Alberto Korda, is one of the most ubiquitous images of our time, appearing on a seemingly endless parade of merchandise from t-shirts to tea towels and everything in between. The Victoria & Albert Museum in London believe it to be the most reproduced in human history while Jonathan Green, director of the California Museum of Photography has speculated that it "has worked its way into languages around the world. It has become an alpha-numeric symbol, a hieroglyph, an instant symbol."

In my youth, like almost every teenager experiencing the hormonal frustrations of adolescence, I too displayed the famous "Che" poster featuring the Cuban flag above my bed. I knew little of the man depicted or what he stood for, only that people thought he was pretty cool and that he had a nice beard. I bought it though as a metaphorical two fingers to the oppressive regime of my parents, with their cruel policies of enforced fruit and vegetable consumption and 11pm curfews. I wasn't going to give in to "the man", man, and this poster proved it.

It didn't work. Mum thought it was Robert Lindsay.

Futile as my protest was, it goes to show just how far Guevara's likeness has been removed from his beliefs. So much so that both are now rendered utterly pointless. There is now even a dedicated "Che" online superstore (www.thechestore.com) where you can buy "officially licensed" merchandise. Just quite who has the authority to licence such goods is unclear, but what is known is that the website is based in the USA and priced in US Dollars...just as he no doubt would have wanted.

So what use is a communist revolutionary who promotes consumerism? And what good are the products encouraging anti-capitalism?

Hours before his death, Guevara asked to see the headmistress of the school which had become his makeshift prison, 22 year old Julia Cortez. During their brief conversation he pointed out the poor condition of the schoolhouse, stating that it was "anti-pedagogical" to expect students to be educated there, while "government officials drive Mercedes cars", declaring "that's what we are fighting against." Forty years later, at the launch of a new car-sharing scheme in Las Vegas (not ordinarily known as an especially socialist town), Mercedes displayed an adapted version of "Guerrillero Heroica" as it's backdrop, the revolutionary star on Guevara's beret crudely replaced by the Mercedes logo. Truly the detachment was complete.

For Fawkes it is no different. For centuries his effigy has been burnt in celebration of his riddance but today it is sold in fancy dress shops up and down the land, acting too as the defining icon for the Hacktivist's darlings – Anonymous.

What began as a digital witch hunt has developed into a genuine world power. Time Magazine named the group amongst its 100 most influential people in the world in 2012, despite no-one knowing who the vast majority of its members actually are. Their faces are hidden behind a mask – the smiling face of Fawkes stylised by David Lloyd for the DC Comic "V for Vendetta". The story focuses on one vigilante's efforts to bring down an authoritarian British government in a dystopian fictional future. When developing the vision of the eponymous "V", Lloyd wrote a handwritten note:

"Why don't we portray him as a resurrected Guy Fawkes, complete with one of those papier-mâché masks, in a cape and a conical hat? He'd look really bizarre and it would give Guy Fawkes the image he's deserved all these years. We shouldn't burn the chap every Nov. 5th but celebrate his attempt to blow up Parliament!"

In the context of the comic the analogy with Fawkes is more than valid, both operated towards similar aims whilst using similar questionable, and often violent, methods. For Anonymous however the link becomes tenuous at best. Since their formation 9 years ago on the forum 4Chan, the self-appointed and self-regulated guardians of the internet have racked up a lengthy list of victims. Their iconography can be seen across the globe from Berlin to Bahrain, websites have been brought down, buildings occupied and viruses spread – all in the name of internet freedom.

On 5th November 2013, celebrated in the UK as Guy Fawkes Night, Anonymous rallied its "legion" to take to the streets, each one sporting the "V" mask, to protest against … well, anything they liked really. Like my teenage affinity to Che the icon, the differentiation between Fawkes the man and Fawkes the smiling mask seemed unclear for those protesting, as did the notion of a common focus for the protests. Various targets were singled out by the "Million Mask March" including the NSA, fracking, rising food costs, energy bills, the FIFA World Cup, banker's greed, corporate greed and the continued presence of Noel Edmonds on British Television (I might have made the last one up).

One of a number of Facebook pages for the event described it as a "Call for Anonymous, Wiki Leaks, the Pirate Party, Occupy and Oath Keepers to defend humanity". In the UK, as protesters inevitably clashed with police forces in Parliament Square and hurled fireworks at Buckingham Palace it appeared they were doing anything but. Unsurprisingly, a movement based on anonymity and unlawful hacking appears to have been hijacked itself for the ulterior motives of less altruistic individuals.

As much as they claim to the contrary Anonymous have not yet changed the world. Nor will they ever in their current, anarchical, state. Without concentrated effort and reasoned argument, their causes, whether noble or not, will remain unsolved. To date all that has been achieved is bringing an acceptable face to unacceptable bullying and fear. A fictional character fighting fictional enemies has become real life extremists fighting real life people, yet no one blinks an eye.

The inconvenient truth is that Anonymous' rise in notoriety owes more to its PR machine than its ideology. Without the mask, the mantra and the glamorised publicity their protests would be seen in a similar vein to the London riots, merely the work of opportunist trouble makers. Their attacks rarely have an established point, focus or goal. They appear to take up causes on a whim and then approach with a brute force mentality, determined to destroy all in their path regardless of whether guilt has been established first. Make no mistake, much of the work carried out in Anonymous' name is terrorism. It may not involve hijacking planes or blowing up Parliament but the threat and chaos is just as great. How many of their "legion" would be as willing to act in their name if they weren't afforded the privacy of the mask – forced to reveal their identity and accept the consequences as the man whose face they bear did?

Anonymous has the opportunity to be a genuine force for good, to usher in a new generation of politics that focuses more on issues that matter to the populous in way which resonates with the next generation. But therein lies the problem. Guy Fawkes is to Anonymous what Che Guevara is to Mercedes Benz, simply a clever marketing device, a pretty picture that can be easily appropriated - and while that remains the case, change can never come.

CARM

POST BREACH SECURITY: CARM AFTER THE STORM

Data breaches create fear within organisations and as a result, everything about an organisation's security strategy has always been focused on stopping breaches from happening.

The inconvenient truth is that breaches continue to happen. In fact, data breaches are becoming frequent and increasing in severity, and therefore we must accept that it is not a case of *if* a business will suffer a data breach as a result of a cyber attack, but simply *when*.

Breaches can be malicious or non-malicious but whatever the intent, any exposure or theft of business data, operational disruption or the 'brand impact' is extremely costly. As a result, organisations are finding it increasingly difficult to invest in preventative measures, and still continue to be challenged around the post-breach scenario. With the volume of attacks causing a big data problem, it is left to un-skilled employees to address the issues but still no one to clear up after the attack has taken place. Unfortunately, this is allowing response times to be too long and insufficient resources are delaying the appropriate remediation. It seems that little effort is left to complete a forensic study, or develop the regulatory/compliance reports, and managed mitigation is a fantasy.

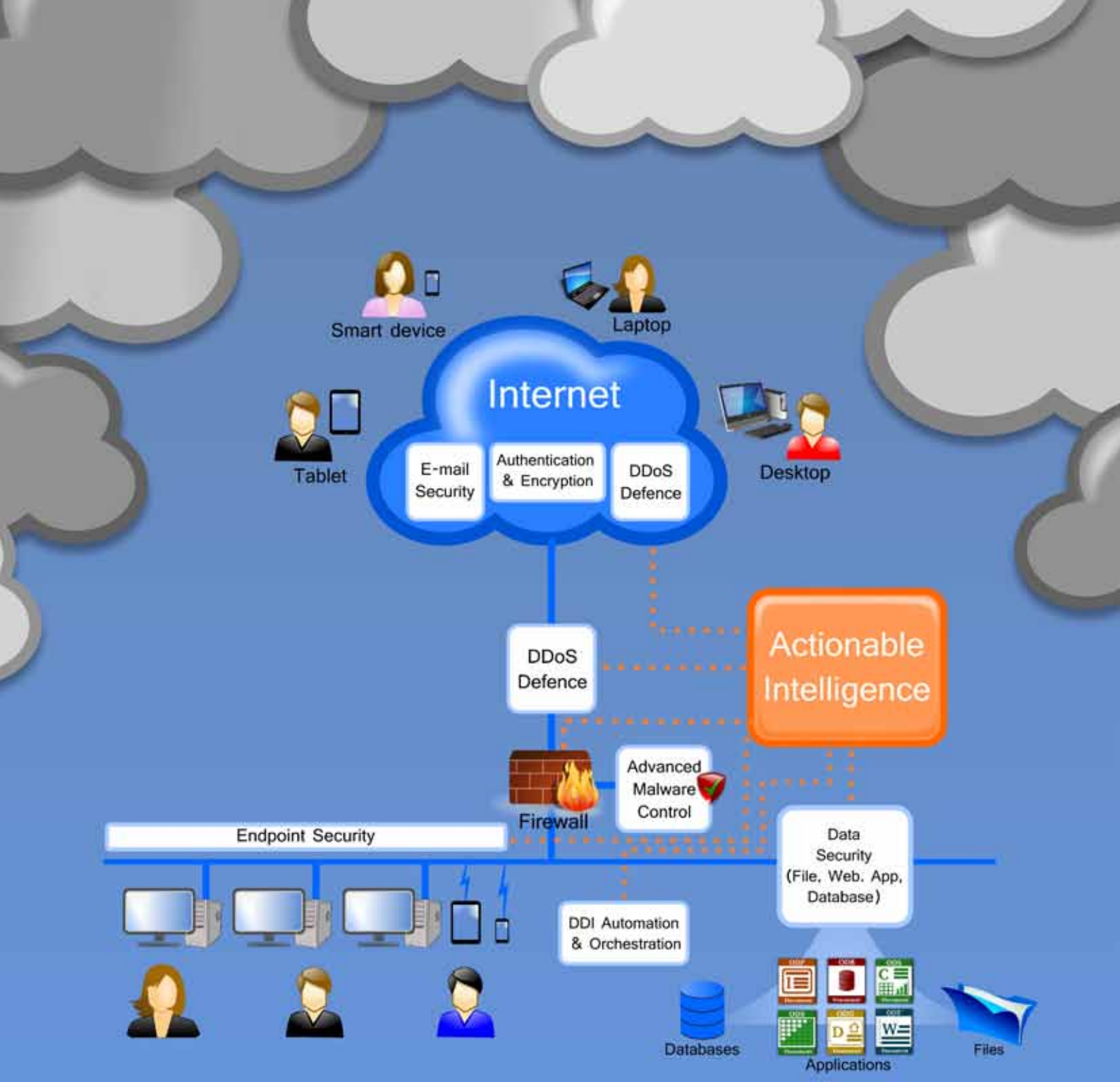
This has been the impetus for CARM (Cyber, Attack, Remediation and Mitigation), a platform capable of addressing the post breach issues organisations face following a successful cyber attack. CARM adds reaction to your existing detection and protection topologies. By implementing a process of detection, identification and remediation, CARM downgrades successful attacks into known threats.

By combining the best of breed capabilities of numerous vendors such as LogRhythm, Infoblox, FireEye, Palo Alto Networks, Bit9, Imperva, Mandiant and Fortinet, CARM helps address the key issues facing CISOs; lack of visibility, volume of incidents, classification of incidents, time to detect, time to contain and ultimately the minimisation of the attack's impact.

It seems that little effort is left to complete a forensic study, or develop the regulatory/compliance reports, and managed mitigation is a fantasy.

The real beauty of CARM is its flexibility to integrate even further with existing legacy vendor technology already deployed. Whether that's firewalls, IPS, anti-malware etc., this means existing investments are not dead. CARM does not 'rip and replace' but instead leverages previous investments which were designed for prevention purposes, to deliver a post-breach solution. And with CARM available to demonstrate as a live working platform, organisations can trial and build various scenarios to test the automation and rapid remediation benefits.

- Quicker response, lower breach impact
- Better, more isolated breach fixes by virtue of its early warning system
- Easier, faster breach notification and forensics in spite of big data
- Fewer IT hours, no human error thanks to maximum automation
- Remediation learning eliminates repeat threats
- Significantly more cost effective than adopting multiple technologies through any other model



With the volume of attacks causing a big data problem, it is left to un-skilled employees to address the issues but still no one to clear up after the attack has taken place.

The changing face of the security landscape is increasing the need for post-breach security and this is happening at the same time as innovative security vendors are coming to market with highly capable post-breach solutions. The CARM initiative is a way of making that process as easy for the market to adopt as possible.

If your organisation isn't thinking about the post-breach scenario then 2014 is the year to think differently. You already want to minimise costs in your business, so minimise the costs of an inevitable security breach! Turn your attention to building capabilities that shorten the time to detect a breach and the time to contain it. Time is money; the longer a breach remains open, the more it will cost the business.

CYBER SECURITY IN THE BUILT ENVIRONMENT

HUGH BOYES

CENG FIET CISSP

IET SECURITY LEAD

Economic and environmental pressures coupled with rising public expectations have led to rapid development of technology in the built environment.

These developments are manifest in the increasing automation of systems and integration of their control systems, with such buildings referred to as smart or intelligent. The best examples of these buildings are often found in public facilities such as stadia or airports. This increasing complexity and integration is not without risk, and these locations represent attractive targets for hacktivists, criminals and terrorists.

The Barcelona El Prat Airport is a good example of how the deployment of integrated and centralised control platforms has revolutionised management of a complex environment. The airport invested in this technology to enable expansion to manage the 29 million passengers and over 100,000 tons of cargo that pass through it annually. The airport uses a single control platform to manage the building management systems for two terminals, support flight operations, control and monitor power plant, support the automated luggage transport system and a number of ancillary services, e.g. water and waste management, police and fire brigade.

To appreciate the scale of the operation, this control platform integrates over 20 different technologies, processing over 700,000 signals through 80 servers. One of the terminals has over 33 technical climate rooms, 1000 fancoil units, 650 fans, 250 mechanical transport items (e.g. escalators, lifts, etc), 247 major plumbing items (e.g. pumps, valves, etc), a complex lighting system comprising over 10,000 managed components and some 30,000 controlled fire detection items. These complex control systems are operated using redundant servers located in the airport's two geographically separated data centres. The system is designed to automatically failover in the event of a power failure in one of the centres.

These airport control systems are typical of the complex cyber physical systems that are being deployed in the built environment. These solutions are not limited to single sites like airports or stadia. In the German city of Bremen, the local authority uses a central control platform to oversee the operation of the building management systems in over 160 facilities. The Bremen solution has simplified the training of operators as they no longer need to be trained on individual systems and also achieve an energy saving of between 15% and 18%.

In common with other distributed computer-based systems, these complex cyber physical systems are vulnerable to a wide range of cyber security threats. In the past many industrial control systems (ICS) or SCADA (Supervisory Control and Data Acquisition) systems appeared to rely upon security through obscurity. Programming of ICS controllers (PLCs - Programmable Logic Controllers) and SCADA human machine interface (HMI) required specialist knowledge. The situation has changed with the discovery of malware like Stuxnet, Flame and Duqu which are targeted at the components used in industrial control systems. These infections may be spread unintentionally through technicians and support staff using USB sticks or personal computing devices, through poorly protected Internet connections, or as a malicious attack.

The problem is not confined to large public buildings or complexes like airports. With the trend towards home automation, including smart meters and computer-based systems managing energy and water consumption, our homes and offices will be exposed to cyber security threats. These innovations often rely upon common technologies or platforms and typically include wired or wireless connectivity with minimal security protection. The lack of protection is likely to get worse as the Internet of Things becomes a reality, as this will involve a wide range of battery-powered sensors employing lightweight protocols to minimise power consumption and thus extend battery life.

To address the increasing threats to the infrastructure supporting our lives and businesses, we need to start taking vulnerabilities very seriously. The key vulnerabilities that need to be addressed are:

- Increased exposure – the use of communications and computer networks to link devices provides more access points thus increasing the exposure of systems to potential attacks or interference;
- Interconnectivity – the interconnection of systems and creation of systems-of-systems creates a greater range of interactions and introduces new paths for attackers or malware to exploit, pathways to allow movement between systems, and increased risk of unintentional spillage of sensitive data;
- Complexity – the evolution of systems-of-systems creates complex interactions, where an incident or failure can have significant impact or lead to a cascade effect in linked systems;
- Common computing and communications technologies – the adoption of common commercially available technologies means that any weaknesses have a widespread impact;
- Increased automation – as human interaction is increasingly replaced by automated controls, there is a risk that unusual or unplanned combinations of events may result in system failure or in an operator making a poor decision.

The interconnectivity and complexity issues identified above can also contribute to an increased privacy risk. For example, the automated collection of data about user behaviour, location, purchases, images, etc. may lead to situations where significant volumes of personal identifiable information are at risk. Extensive interconnection of systems allows data to be accessed, processed or stored by an increasing range of systems, with a consequential loss of control or privacy breaches. For example CCTV feeds are often handled over digital networks, allowing the images to be monitored at remote locations, but also creating the risk of inadvertent routing/patching to incorrect destinations.

To address the vulnerabilities we should take steps to address the cyber security of industrial control systems (ICS) used in the built environment and to improve the trustworthiness of both software and systems. The Trustworthy Software Initiative [http://uk-tsi.org/] is already developing the knowledge base and an awareness programme to encourage the development of trustworthy software. These principles need to be adopted in the design, production and operation of building management systems. The UK Government is planning investment in a Trustworthy ICS Research Institute, to be launched next year; this should help focus research in this important area. The Institution of Engineering and Technology (IET) has published a free downloadable document addressing key issues related to "Resilience and Security of Technology in the Built Environment" – see the IET website [http://www.theiet.org/resources/standards/ cyber-buildings.cfm]. Following on from this, an IET working group is now developing a "Code of Practice for Cyber Security in the Built Environment", which should be available in mid-2014. The IET is also working with the BCS, the UK Government and academia to explore how an awareness of cyber security issues may form part of all accredited UK degree courses, so that our future workforce has a greater appreciation of the issues.

You can take steps to protect your business premises and offices by considering the vulnerabilities in your building's infrastructure and systems. You should be concerned about whether your facilities management team and their contractors are practicing good cyber hygiene to reduce the risk of malware infection of building systems. You should also consider putting in place a cyber security awareness programme for all of your employees and contractors, to reduce the risk of cyber security breaches from insiders. Don't assume it will not happen to you, if your building systems are poorly protected it is only a matter of time before a weakness is exploited. Building systems are already being compromised, so act now and avoid becoming another statistic.

CYBER CRIME AND WARFARE

REVIEWED BY PROFESSOR TIM WATSON

DIRECTOR OF CYBER SECURITY CENTRE WMG, UNIVERSITY OF WARWICK

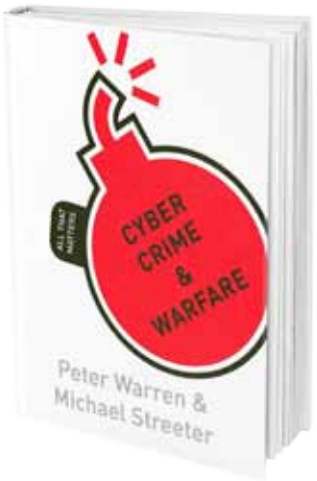
Everyone is aware of cyber crime now. From sensational headlines in the national press about internet-connected smart fridges delivering malicious emails, and threats to our critical national infrastructure from terrorist hackers, to sinister stories of international crime gangs stealing millions from banks and controlling armies of zombie computers, the digital realm is seen as a lawless Wild West frontier as much as it is a brave new world of big data and smart devices, providing help and prosperity to individuals, communities and organisations around the world. But how can the general reader, the school or university student or the busy decision-maker tell fact from fiction? How can the issues in this rising tide of digital attack and defence within the cyberspace be grasped?

In their clear, accurate and illuminating book, Peter Warren and Michael Streeter have provided a concise handbook for anyone interested in the dark world of cyber crime and warfare. With a journalist's eye for a good story and an excellent grasp of the technical essentials, this gem of a book covers a wide range of topics succinctly and accessibly but with enough depth to provide the reader with sufficient understanding to form their own opinions on the issues raised. The numerous facts are well chosen and accurate. The boxed summaries of key concepts are very helpful. In spite of the book being published before the publicity surrounding Edward Snowden and the revelations concerning the extent of state surveillance, the book is a comprehensive and up-to-date account of cyber crime.

The book starts by analysing the nature of cyber crime and then moves on, chapter by chapter, to cover the history of hacking, the rise of the Internet and the virus threat, industrial cyber espionage, identity theft and the curse of spam, the rise of botnets, cyber criminal profiles, policing cyberspace, cyber crimes targeting children, cyber warfare and future technology. The book finishes with 100 ideas that can be used to explore the subject in more depth: cyber crime websites, places of hacking pilgrimage (although I'm not convinced that I shall be carrying my stick and scallop shell on the trail that leads to the door of Gary McKinnon!), hacking conferences, films and books on cyber crime etc. Although the book covers some tough topics they are handled sensitively and I see no reason why this book could not be used in secondary schools as well as in universities.

This is a small book but all the better for it. I have read books several times larger that have contained only a fraction of the information and insight provided by Warren and Streeter. If you are looking for a short book that shines a light on the dark side of cyberspace then I can think of no better book to recommend than this one.

MARKS OUT OF 5	*5 out of 5*
REVIEWER NAME	*Professor Tim Watson*
BOOK TITLE	*Cyber Crime and Warfare*
BOOK SERIES	*All That Matters*
AUTHORS	*Peter Warren and Michael Streeter*
PUBLISHER	*Hodder & Stoughton*
DATE OF PUBLISHING	*2013*
ISBN	*978-1-4441-8998-8*
PRICE	*£8.99*



Cyber WEEK REVIEW

By Helen Morgan, SBL

The launch of the De Montfort University (DMU) Cyber Security Centre in September 2012 was a significant milestone in the teaching and research of cyber protection.

Building upon the success of the first year since the launch of the Cyber Security Centre (CSC), this year the CSC Annual Conference was combined with a number of new events to form DMU Cyber Week 2013.

Taking place from Monday 16th – Thursday 19th September 2013, the series of events brought together an international community from the public and private sectors, law enforcement, academia, defence and the third sector and provided a unique opportunity for delegates to gain a fresh understanding of issues that really affect the cyber domain and the different approaches and solutions that are available to protect this environment.

The week began with the First International Symposium on Industrial Control System & SCADA Cyber Security Research (ICS-CSR2013) organised by DMU's Software Technology Research Laboratory and the European Aeronautic Defence and Space Company (EADS-IW). The event was a great success in balancing industry needs and cutting edge research in this increasingly important area.

Conference organiser, Helge Janicke said: "We are pleased with the high-quality of the research contributions and indeed the interaction during the conference. We are delighted to be working closely with EADS on research to establish how ICS and UK businesses are exposed to cyber-threats and how the right information about these systems' security behaviours can be made available to decision makers as part of the EADS Centre of Excellence in SCADA Cyber Security & Forensics here at DMU."

John Alexander exhibited his extensive collection of cryptography machines, some predating WWII and one which had been salvaged from the ocean floor! His collection showed the development of this technology over the past 80 years.

The cryptography exhibition was enjoyed by those attending the Inaugural Meeting of the East Midlands Branch of the Institute of Information Security Professionals (IISP). Twenty-five delegates were treated to a presentation and demonstration by Jay Abbott, Managing Director of Advanced Security Consulting Limited on how easy it has become to play the role of the bad guy in cyber security.

Following the presentation a discussion focused on how security professionals can focus the attention of businesses on the reality of threats and the investment needed to protect against them.

Colin Robbins, Technical Director at Nexor said of the meeting: "As professionalisation of cyber security grows, regional networks will become key to enable local practitioners to share ideas and good practice. It was great to see there was sufficient interest to launch such a network, under the IISP banner, in the East Midlands."

Cyber Week concluded with two conferences on Thursday 19th September.

The First Annual Cyberpsychology Conference organised by Alison Attrill and her team in the Psychology department at DMU featured keynote speaker Professor Monica Whitty from the University of Leicester. The day was packed full of presentations and seminars on a range of topics under the Cyberpsychology umbrella.

The conference also featured a presentation of posters, some of which were written by PhD students and gave the delegates an opportunity to network and discuss findings and ideas.

Event organiser and Senior Lecturer in Psychology, Alison Attrill said: "This first annual event was very successful in bringing together delegates from wide and varied backgrounds to present on diverse topics revolving around online behaviour."

The final event of the 2013 Cyber Week was the Cyber Security Centre Annual Conference. Delegates were welcomed to the event by Director of the CSC, Professor Tim Watson who talked through some of the Centre's achievements since the launch in 2012.

Keynote speaker, Neil Kenward, Deputy Director, National Cyber Security Programme for the Cabinet Office emphasised the importance of academia in providing cyber security training and research.

He stressed the value of partnerships between universities and businesses and highlighted DMU's Cyber Security Centre as an example of the high-level collaborative approach that is required to help the UK remain at the forefront of cyber security developments.

Mr Kenward said: "Academia is a vital provider of research and knowledge in this fast moving field and critically, they are the producers of the essential cyber skills the UK needs.

"We are keen to encourage businesses and universities to work together, to ensure that the research and training provided by the educational sector is focused on the requirements of British business. De Montfort University is an excellent example of how to make such collaboration work in practice."

Between presentation sessions, delegates at the CSC Annual Conference were also invited to look around a vendor exhibition that showcased the latest products and services from the IT industry.

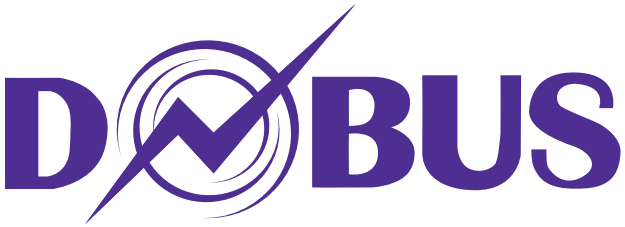
Since its launch, the Cyber Security Centre has become involved in numerous projects including the Trustworthy Software Initiative (TSI) that is hosted by the CSC. The TSI is a prestigious research initiative, and has been recognised by Government Minister Francis Maude who said: "We support the Trustworthy Software Initiative, which aims to improve cyber security by making software more secure, dependable and reliable, and to educate on why trustworthy software is important."

In addition to the TSI, the Cyber Security Centre has also been recognised as one of four centres of excellence for cyber security in the UK by the Institute of Engineering and Technology, and has launched a new Master of Science degree in Cyber Security in collaboration with Deloitte, with Cabinet Office Minister Chloe Smith praising the 'vital' work of De Montfort University.

Professor Tim Watson, Director of the Cyber Security Centre, commented that "It was exciting to see so many different events and activities during DMU Cyber Week. It highlighted the breadth of cyber research across all faculties and the strength of the links between research groups and their partners in industry, with other academic institutions and with professional bodies and government organisations."

Following the success of this year's DMU Cyber Week, dates are already being put in place for Cyber Week 2014. If you would like to be involved in next year's event, please email DMUSecretariat@softbox.co.uk for more information.

Proceedings from the First International Symposium on Industrial Control System & SCADA Cyber Security Research are available at: www.bcs.org/ewic/ics-csr2013.



To Find Out More Contact:
01347 812100
cloud@softbox.co.uk
www.softbox.co.uk

SBL's portfolio of Cloud Services are designed to accommodate security and assurance concerns inherent within Public Sector Cloud adoption strategies via the utilisation of firstly; a UK Secure Facility Hosting Environment (Safe Harbour), and secondly SBL's High Security and Award Winning DOBUS™ Platform employed as a central delivery mechanism to Public Sector and Private Networks.

DOBUS™ enables the delivery of real time, clean, and verified patches to end-point Security, Infrastructure, and Application Software over a secure bearer. The DOBUS™ service operates 24x7x365, performs at 99.999% uptime, and has received over 18 million visitors in the last four months alone. It delivers critical patches (e.g. anti-virus signature updates) independent of the internet through secured links into Vendor laboratories, and therefore protects users from the threats posed by website spoofing, and the issues of download location over-subscription, both common characteristics within major malware events.

This unique and innovative service has been delivered via a highly robust, highly accredited, and highly versatile architecture. Various research projects and pilots are currently underway to scope the delivery of the next generation of Community Cloud Services via the DOBUS™ platform. These will include Secure Email and Rights Management Services, Hosted Collaboration Environments, Digital Certificate Issuance Services, Secure File Transfer and On-line Backup services and many more.

The traditional DOBUS™ service is a non-internet reliant, resilient, high availability trusted managed system for the secure provision of software updates, service packs, patches and fixes. Since its inception DOBUS™ has successfully delivered in excess of 21 million individual downloads across one Government department's infrastructure.

In addition to a newly developed comprehensive range of secure patch management solutions, SBL's new Cloud Services include secure Cloud-based Backup, Archive and Recovery as well as Collaboration tools.Additionally, DOBUS™ is expanding its reach onto the UK PSN (Public Service Network), delivering the trusted services the MoD have been relying on for years to many more public sector organisations.

ALMANAC of EVENTS

MARCH

CYBERSECURITY SYMPOSIUM 2014
4th March 2014
Washington DC, USA

INFORMATION ASSURANCE PRACTITIONERS' EVENT
5th - 6th March 2014
York, UK

CYBER INTELLIGENCE ASIA 2014
11th – 14th March 2014
Singapore, Singapore

APRIL

INFOSEC WORLD CONFERENCE
7th – 9th April 2014
Florida, USA

IEEE SOSE 2014
7th – 11th April 2014
Oxford, UK

CYBERPATTERNS 2014 IN CONJUNCTION WITH SOSE 2014
7th – 11th April 2014
Oxford, UK

INFOSECURITY EUROPE
29th April – 1st May 2014
London, UK

CYBERSEC 2014
29th April – 1st May 2014
Beirut, Lebanon

MAY

ISPEC
12th – 14th May 2014
Fujian, China

GOVSEC 2014
13th – 14th May 2014
Washington DC, USA

NISC
14th – 16th May 2014
Glasgow, UK

CEIC 2014
19th – 22nd May 2014
Las Vegas, USA

JUNE

PSN SUMMIT
25th June 2014
London, UK

CYBERTALK

Call for Articles

For CyberTalk #5

The Editorial Board of CyberTalk magazine are currently inviting the submission of articles for Cybertalk #5

If you would like to contribute, please email CyberTalk@softbox.co.uk with a title and short article synopsis no later than 18th April 2014.

Articles will be due for submission no later than 2nd May 2014 for publication June 2014.

Find out more and read past issues online for free at:

www.softbox.co.uk/cybertalk

Join the Debate

Follow CyberTalk on Social Media and receive exclusive benefits inclusive early access to the latest editions

- Facebook.com/cybertalkmagazine
- YouTube.com/CyberTalkUK
- Twitter.com/CyberTalkUK
- CyberTalk@softbox.co.uk
- Pinterest.com/cybertalk
- www.softbox.co.uk/cybertalk

01347 812100
Cybertalk@softbox.co.uk
www.softbox.co.uk/cybertalk