FIGHTING THE COMMON ENEMY:
ADDRESSING THE REAL-WORLD RISKS OF CYBERSECURITY

by Dr Jim Kent
Global Head of Security and Intelligence
CEO, North America
CONTENTS

Executive Summary .......................................................... 3
The Real-World Risks of Cybersecurity ............................ 4
  Cyberattacks on Physical Infrastructure ....................... 4
  Cybercrime Funding and Enabling Terrorism ............... 5
Seeing the Whole Picture ............................................... 6
  Barriers to Sharing.................................................. 6
Integration Efforts in Policy and Technology .................. 7
  Government Moves Towards Information Sharing ....... 7
  Technology to Take Down the Barriers ...................... 7
  Effective Intelligence Sharing ................................. 7
About the Author .......................................................... 8
About Nuix ............................................................... 8
References ................................................................. 8

Making threat information accessible and easy to share among intelligence, investigative, and operations personnel will deliver a unified way to fight the common enemy
EXECUTIVE SUMMARY

Cybersecurity is usually discussed as a threat to our personal or organizational finances. Credit card fraud, online scams, and intellectual property theft are easy money for cybercriminals, who are unlikely to face legal consequences. Likewise, cyberespionage is a relatively easy and low-cost way for nation states to acquire high-value intelligence. There is relatively little discussion on the risks of cyberattacks on physical infrastructure or the growing role of cybercrime in the operation and funding of terrorist groups—but the dangers are real and growing.

Whatever threats they are trying to defend against, three broad groups of individuals and organizations are involved in defeating cybercrime:

- **Intelligence agencies** that build profiles and attempt to predict or pre-empt criminal activity
- **Incident response investigators** from the public and private sectors, who clean up after an event
- **Network operations centers** that manage and monitor security infrastructure to prevent or quickly detect breaches.

All these groups are trying to fight a common enemy but don’t talk to each other due to cultural and technological impediments. I believe it is well past time that we overcome these blockages so society can better address the serious threats of cybercrime and cyberterrorism.

Government agencies in the United States and worldwide are developing the frameworks for better sharing intelligence about cyber-threats. It’s now the turn of security technology vendors to abandon their failed traditional approaches. We must use technology and human brain power effectively, allowing each to play to its strengths. Making intelligence accessible and easy to share among intelligence, investigative, and operations personnel will deliver a unified way to fight the common enemy.
THE REAL-WORLD RISKS OF CYBERSECURITY

The overwhelming focus of discussions around cybersecurity relate to protecting money and valuable information. These are the primary target for cybercrime and cyberespionage activities. Private data and financial information are easily monetized on the black market and often very poorly protected. Intellectual property and national secrets are often also easy to access and steal.

However, cybercrime can hurt us physically as well as financially. There is an ever-present possibility of cyberattacks affecting physical infrastructure in a way that could harm hundreds or thousands of people at a time—or more. In addition, terrorist groups are using cybercrime as an enabling technology for their activities and to raise funds.

Cyberattacks on Physical Infrastructure

Information theft is the major focus of organized cybercrime gangs and state-sponsored cyberespionage units. However, it is within the capabilities of the more sophisticated among both these groups to use malware and hacking techniques to affect real-world infrastructure and physical objects.

The Stuxnet virus, dubbed “the world's first digital weapon,” demonstrated it was possible for malware to have physical effects. It was very specifically engineered to reprogram the industrial control systems that ran centrifuges at an Iranian uranium enrichment facility. Stuxnet achieved its goals even though the control systems it targeted were on a separate “air gapped” network not connected to the internet.

Many supervisory control and data acquisition (SCADA) industrial control systems are highly vulnerable to cyberattacks because their designers assumed these systems would never be connected to a public network. These vulnerabilities have been known at least as far back as 2001, when an Australian man hacked into the SCADA systems controlling the Maroochy Shire sewer system, causing millions of gallons of raw sewage to spill into waterways.

As technology becomes more ingrained and deeply embedded in many aspects of our lives, it also becomes a more serious risk to our wellbeing.

As technology becomes more ingrained and deeply embedded in many aspects of our lives, it also becomes a more serious risk to our wellbeing. Many “internet of things” devices have not been designed for security and contain fundamental flaws. For example, hackers have remotely taken control of a Jeep Cherokee while it was on the road by exploiting flaws in the car’s entertainment system and its connections to the vehicle’s control systems.

Without wishing to give credence to conspiracy theories, it is plausible that the disappeared Malaysian Airlines flight 370 could have been hijacked either on board or remotely by tampering with its flight control systems. For example, security researchers have claimed for many years that it is possible to exploit the Aircraft Communications Addressing and Reporting System used to transmit diagnostic messages between aircraft and ground stations to compromise a plane’s flight management systems.

My question is, given the known vulnerabilities of so many technology systems that we trust with our lives every day—from power stations to pacemakers—why aren’t more of these attacks happening? The nightmare scenario is that a criminal or terrorist group has already infiltrated multiple systems and installed zombie-style malware, which is now waiting for the signal to conduct a coordinated attack.
THE REAL-WORLD RISKS OF CYBERSECURITY cont

Cybercrime Funding and Enabling Terrorism
While the risks of cyberattacks on real-world infrastructure have so far not proven a danger to many people, cybercrime is making us much more unsafe in another way. It provides direct funding for terrorist groups such as ISIS. ISIS also exploits the online medium to impose fear, disseminate propaganda, and recruit new members.

Terrorist groups have been opportunistic about their sources of funding. Drug trafficking has provided cashflow for terrorist groups throughout the world and drugs have even been used as currency in the commission of terrorist attacks, such as in the Madrid bombings. ISIS has also made money from oil production, looting, bank robbery, taxes and selling historical artifacts.

Terrorist groups have conducted increasingly complex cyberattacks as technology has evolved. There is a clear path of escalation, starting with basic attacks such as a white supremacist who temporarily disabled an internet service provider in 1996 and growing to sophisticated hacks such as that conducted by the Free Syrian Army against Australian domain name registrar Melbourne IT.

ISIS’s very effective use of the public web and social media to distribute propaganda is well known. However, ISIS also uses Bitcoin and other cryptocurrencies to transfer funds untraceably and “dark web” forums to communicate with militants and sympathizers. Based on my discussions with the intelligence community, I believe ISIS conducts more than 80% of its recruitment activity on the dark web.

It is also clear that cybercrime is a real money-spinner; the combined global trade in hacking tools, hacking services, and stolen data is likely more profitable than the illegal drug trade because it has more direct links to end-users and the production and distribution costs are negligible. A competent hacker can earn at least US$84,000 per month using off-the-shelf tools, according to one security firm.

Cybercrime would offer “attractive sources of financial gain for [terrorism] financiers, given the opacity of online transactions, the accessibility of means of cybercriminal activity, and the limits of legal and regulatory “reach” in most jurisdictions to investigate, prosecute and prevent financial crimes in cyberspace,” according to non-profit research organization The Fund for Peace.

There are several precedents for cybercrime funding terrorism. Bali bomber Imam Samudra claimed to have funded the attacks through credit card fraud; Indonesian police said they found evidence Samudra tried to do this but not that he succeeded. In 2007, British police arrested 21-year-old biochemistry student Tariq al-Daour and two accomplices, who used phishing schemes and malware to steal credit card details with which they raised more than US$3.5 million for jihadists.

We also know that cybercriminals are recruiting insiders to provide access to company systems and data. According to a recent survey of 4,000 people, more than one-third (35%) of employees said they’d be willing to sell company data for the right price — 22% said they felt no responsibility for their company’s data.

I believe these trends will combine to create a very serious cyberterrorist threat, as shown in Figure 1, which will become more apparent as ISIS’s other sources of funding dry up.
The risks I have described in this paper mean there is a lot more at stake for cybersecurity than companies’ reputations or share prices. Three main groups seek to address cybersecurity threats to our financial and physical wellbeing:

- **Intelligence agencies** that gather information about relationships and use this data to build intelligence profiles and predict or pre-empt major events.

- **Incident response investigators** who may be law enforcement officers, employees, or consultants. They examine much of the same data as intelligence agencies but their interest is in the forensics of who did what and when. They are usually focused on putting out fires or getting things back up and running. They often lack the time, bandwidth, and mandate to proactively discover what is causing the problems.

- **Network operations centers** are primarily concerned with ensuring security systems are up to date and functioning correctly. They monitor network activity and log files to prevent breaches or detect them early enough to take remedial action before they become big problems.

All these groups are trying to fight a common enemy but the specialized nature of their work means they lack a common language. In many cases they don’t talk to each other or aren’t allowed to collaborate. In my experience, the intelligence and investigation communities are often so far apart that even if they are prosecuting the same people over the same event, they probably don’t find out about each other’s involvement until the day of the court case.

The business community is no different. Often companies within a particular industry are targeted by the same groups of cyber-attackers but just try getting them to share intelligence with each other!

### Barriers to Sharing

The barriers to sharing are cultural and technological:

- **Culture.** People are reluctant to discuss if they are experiencing cyberattacks or have suffered a data breach—often for fear of showing weakness or giving up a potential competitive advantage. This is getting better, especially in jurisdictions that have mandatory data breach disclosure.

- **Technology.** Even if organizations can overcome their reluctance to talk about security issues, they lack a standard technical mechanism to share, digest, and apply anonymized threat intelligence.

However, I believe it is possible to overcome these barriers, bring the three disciplines together and achieve a new cybersecurity reality (see Figure 2). By applying technology in new ways and humanizing the data, we can converge the intelligence, incident response, and network operations approaches to become far more efficient in catching the bad guys.
INTEGRATION EFFORTS IN POLICY AND TECHNOLOGY

A lack of integration between the groups attempting to address cybersecurity threats severely hampers their activity. However, there are changes underway at the policy and technology levels.

Government Moves Towards Information Sharing

The US Senate will soon debate the Cybersecurity Information Sharing Act, which aims to make it easier for businesses to exchange details about cybersecurity incidents with the government. The shared information could include customer IP addresses, email headers, timestamps, and other metadata that serves as indicators of a particular threat.

MITRE, a US Federal Government-funded not-for-profit research company has introduced the CyBOX, STIX, and TAXII formats for sharing threat intelligence. However, there is still work to be done on enabling organizations to share this information without exposing themselves.

There are also organizations being set up to aggregate and analyzes suspicious online activity, such as the US Department of Homeland Security's National Cybersecurity and Communications Integration Center and the non-profit Multi-State Information Sharing and Analysis Center.

Technology to Take Down the Barriers

The technology industry must recognize its past faults and forge a new path. Consensus has emerged over the past two years that the traditional “perimeter security” approach to network security has failed. Security experts now believe determined attackers can infiltrate any perimeter security system and lodge malware within organizations’ networks. Gartner’s bluntly titled report, Malware Is Already Inside Your Organization; Deal With It argues that “organizations must assume they are compromised, and, therefore, invest in detective capabilities that provide continuous monitoring for patterns and behaviors indicative of malicious intent.”

Technology vendors have also focused too much on catering to a geeky cybersecurity clientele at the expense of simplicity and usability. We need to move away from the “green type on black screens” model of technology and deliver answers in a more accessible and digestible format. We must apply technology to do the hard work for us and enable smart people to use their brain power and analytical skills more effectively.

Nuix is one technology vendor determined to take down the barriers between the intelligence, investigative, and operations groups of cybersecurity defense. By allowing these disciplines to work together and aggregating information from the deepest forensic detail to the highest relational analysis, we will deliver a unified way to fight the common enemy.

EFFECTIVE INTELLIGENCE SHARING

Nuix is already helping law enforcement, government, and corporate clients around the world share intelligence more effectively—internally and between agencies.

For example, the Attorney-General's department in one country has used the Nuix case file format to share information with its national police force. The police collect and process the data they seize in evidence, then provide the case files to the Attorney-General's department for in-depth analysis.

Another large regional police force has used Nuix investigation technology to tackle serious and organized crime. Our software has made it easy to extract intelligence from digital evidence which can be shared with other police and law enforcement agencies across the country.
Dr. Jim Kent
Global Head of Security and Intelligence
CEO, North America

Dr. Jim Kent is recognized as a global industry leader in information security, incident response, eDiscovery, and digital forensics. He was a pioneering high-technology crime detective in the United Kingdom. Dr. Kent has more than 20 years’ experience as a senior digital forensics investigator, information security consultant, and high-level advisor to the law enforcement, government, financial, and commercial sectors. In 2013, Dr. Kent was appointed as an advisor to the ITU, the United Nations’ cybersecurity body. He co-wrote the UK Association of Chief Police Officers’ digital investigation best practice guide and served as an expert witness in the High Courts of Justice.

Dr. Kent’s hands-on experience has led to his vision for a different way of approaching cybersecurity. He has manifested this vision in the team of security and intelligence experts he has assembled to lead Nuix’s cybersecurity technology, services, and training.

Dr. Kent has developed and delivered a postgraduate curriculum of training in computer security and forensics. He received his Doctorate (Hons) in Science from the University of Bedfordshire and holds numerous professional certifications in digital forensics and cybersecurity.

REFERENCES
ii Tony Smith, “Hacker jailed for revenge sewage attacks”, The Register, October 31, 2001
iv Ben Sandilands, “MH370 computer hack risk underlined by Polish airlines attack”, Crikey, June 24, 2015
v Lucian Constantin, “Researcher: Vulnerabilities in aircraft systems allow remote airplane hijacking”, PC World, April 10, 2013
vi United Nations Office on Drugs and Crime, “Drug trafficking and the financing of terrorism”

ABOUT NUIX
Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

TO FIND OUT MORE VISIT
nuix.com/cybersecurity