

2017 Enterprise Risk Management Symposium

April 20–21, 2017, New Orleans

The Cyberrisk Ecosystem: Where We Are, How We Got Here and Where Cyber Risk Management Can Take Us

By Ben Goodman

The Cyberrisk Ecosystem: Where We Are, How We Got Here and Where Cyber Risk Management Can Take Us

Ben Goodman[1,2]

Abstract

This paper is intended to provide readers with insight into the dynamic cyberrisk ecosystem as it has evolved over recent decades, both from the perspective of the billions of individual and corporate internet users of the "surface web" and from the perspective of the millions of users of hidden services on the "dark web." Just as biological ecosystems include agents that are largely constructive in nature, coexisting with some that are mainly destructive, as well as some that are visible and some that are hidden, this paper attempts to reveal some of the hidden agents and explain some of the interrelationships between constructive and destructive forces that coexist in this complex, dynamic system of cyberrisks.

This paper also reviews some of the major challenges confronting those who seek to manage cyberrisk, and includes suggestions regarding how a richer understanding of the cyberrisk ecosystem can be used to help organizations better manage cyberrisk. The paper concludes with several recent examples of emerging cyberrisks that illustrate the cyberrisk ecosystem at work. These examples also demonstrate significant characteristics of correlated risk. Finally, one insurer provides an example of how embracing these emerging cyberrisks may enable them to seize upon a market opportunity.

Introduction

Not very long ago, cyberrisk was called "network risk" and was largely considered a "technology problem," relegated to information technology departments. Today, cyberrisk ranks as the first or

[1] Ben Goodman is the founder and CEO of 4A Security & Compliance, with over 30 years of experience in information technology, technology strategy and risk management. Ben is a member of the faculty at Drexel University and LeBow School of Business, a recipient of ISACA's Certified in Risk and Information Systems Control (CRISC) Worldwide Achievement Award, a Fellow of the Ponemon Institute and a member of the Pace University, Seidenberg School of Computer Science Cybersecurity Advisory Board.

[2] I would like to thank my sister, Dr. Jacqueline Goodman for her feedback, insight, and editorial assistance. I would also like to thank Paul Rosovsky for his assistance with research, proofing and overall attention to detail. Finally, I would like to thank the members of the Joint Casualty Actuarial Society/Canadian Institute of Actuaries/Society of Actuaries, Risk Management Section for raising awareness and interest, and elevating the dialogue on the topic of cyber risk.

second operational risk in surveys of U.S. and Canadian executives and boards.[3] Globally, cyberrisk is found among the top five overall risks in surveys across business, government and nongovernmental organizations.[4] The potential consequences of cyberrisk events range across a variety of risk categories including regulatory compliance, legal, reputation, vendor and supply chain, and business continuity, as well as risk transfer and insurance. As recent exploitations of vulnerabilities found in Internet of Things devices such as medical devices,[5] motor vehicles,[6] emergency notification systems[7] and energy grids[8] have demonstrated, physical damage and health and safety concerns must now be added to this list as well. Given its broad impact and heightened profile, cyberrisk is of particular importance for chief risk officers and others responsible for monitoring and managing emerging risks.

Despite all the attention and resources applied toward the management of cyberrisk, cyberthreats evolve rapidly and new cyber incidents continue to occur with increasing frequency and severity around the globe. Analysts estimate global cybersecurity spending has grown 35 times in the last 13 years and predict increases in the five-year compounded annual growth rate from 4% to 15% (which would equate to spending of more than $1 trillion by 2021).[9] Even on the low end, these are enormous expenditures, but there is still very little reliable data upon which to model cyberrisk, or to make fact-based decisions regarding the efficacy or "return on investment" of specific cyber risk management initiatives.

Part 1 of this paper surveys the cyberrisk ecosystem as it has evolved on both the surface web and the dark web. A review of some of the fundamental technological developments that have contributed to the rapid rise of cyberrisk follows. These will provide context for Part 2, a discussion of the major challenges confronting those who seek to manage cyberrisk, and includes suggestions regarding how a better understanding of the cyberrisk ecosystem can be used to help organizations turn cyber risk management decision-making into a competitive advantage. In Part 3, three examples of emerging cyberrisks illustrate the cyberrisk ecosystem at work. These examples also demonstrate significant characteristics of correlated risk. Finally, one insurer provides an example of embracing these emerging cyberrisks to seize a market opportunity.

---

3 North Carolina State University, ERM Initiative and Protiviti, "Executive Perspectives on Top Risks for 2017: Key Issues Being Discussed in the Boardroom and C-Suite," 2017 report, *https://www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-2017-top-risks.pdf*.

4 World Economic Forum, "Global Risks Report 2017," *https://www.weforum.org/reports/the-global-risks-report-2017*.

[5]Jim Finkle, "J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," *Reuters*, Oct. 4, 2016, *http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L*.

[6] Andy Greenberg, "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," *Wired*, Aug. 1, 2016, *https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/*.

[7] Eli Rosenberg and Maya Salam, "Hacking Attack Woke Up Dallas With Emergency Sirens, Officials Say," *The New York Times*, April 8, 2017, *https://www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html?_r=0*.

[8] Andy Greenberg, " 'Crash Override': The Malware That Took Down a Power Grid," *Wired*, June 2, 2017, *https://www.wired.com/story/crash-override-malware/*.

[9] Cybersecurity Ventures, "Cybersecurity Market Report," accessed April 25, 2017, *http://cybersecurityventures.com/cybersecurity-market-report/*.

Part 1. The Cyberrisk Ecosystem: Shining a Light on the Dark Web

For most law-abiding internet citizens, the world of cybercrime and the dark web are mysterious and somewhat inscrutable. But just as pathogens may not be visible to the naked eye, cybercrime is a pervasive and ever-present part of our internet environment. We ignore it at our own peril. A basic understanding of both the ecosystem within which cybercriminals operate to attack enterprises and the dynamics that continuously reshape the threat landscape will prove highly valuable to risk managers as they develop strategies to address those cyberrisks.

In many ways, the world of cybercrime on the dark web is a shadowy, yet organic, reflection of the vibrant, ever-changing global marketplace for technical and business products and services on the surface web. Just as commercial enterprises have sought to gain a competitive advantage in the marketplace by leveraging the capabilities enabled by new technology, so too have cybercriminals utilized many of the same tools to build and market new products that exploit the maximum number of victims while staying ahead of law enforcement. Both organized crime and enterprising individual cybercriminals have seized upon a decentralized organizational structure, enabled by the dark web, to implement business models and a sophisticated cybercriminal-to-cybercriminal (C2C) global market infrastructure. Two important technical innovations have served as critical enablers for the thriving world of cybercriminal activity and darknet markets on the dark web: The Onion Router (Tor for short) and bitcoin.

Tor was originally funded by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Naval Research Lab in the 1990s[10] to provide a mechanism for secure, anonymous communication. It was designed to allow messages and interactions to travel on an untrusted network while resisting traffic analysis and eavesdropping. Useful for dissidents and secret intelligence, the naval researchers believed the Tor network would be more effective at hiding communications inside a larger crowd, and, for that reason, Tor was released into the public domain. Today, there are more than 2 million users of the network. Tor also enables "hidden services." These are most commonly websites, darknet markets and chat rooms where users can interact anonymously at locations that remain hidden from surface web search engines like Google but are known to the parties involved in the transactions.

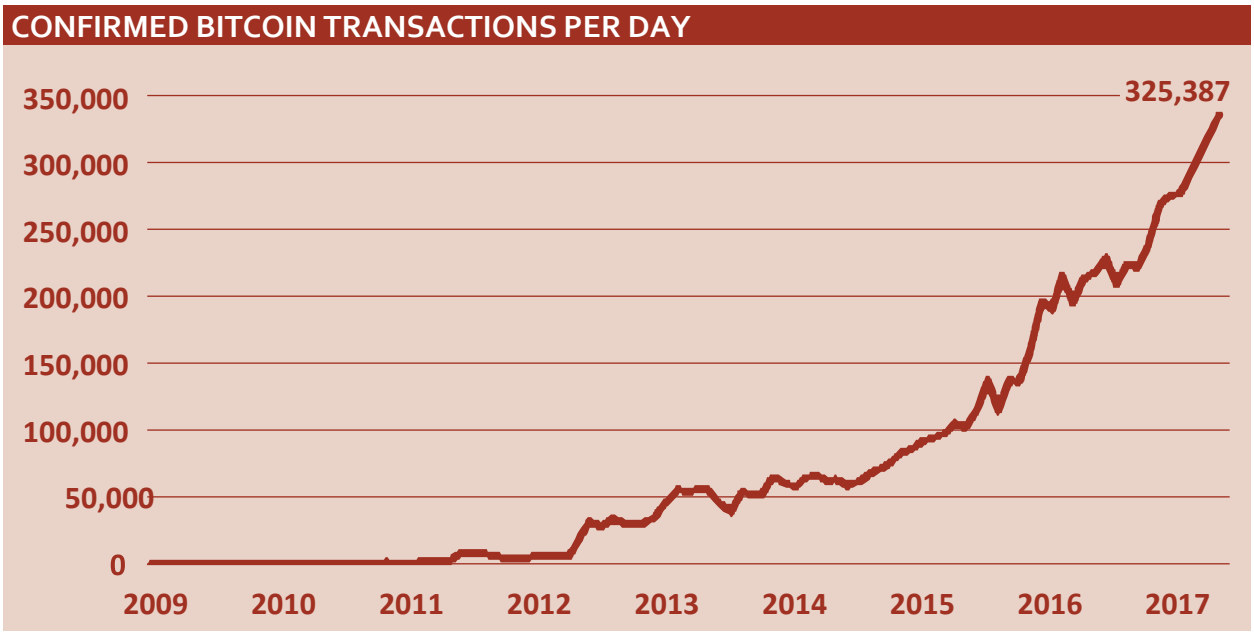
The second innovation critical to the development of cybercrime is a cryptocurrency and anonymous payment system called bitcoin. Bitcoin was released as open-source software in 2009. Bitcoin transactions do not involve any intermediary, central repository or governing administrator. Today, there are more than 325,000 confirmed transactions, totaling about $200 million, daily.[11] It is not possible to determine the exact number of bitcoin transactions that involve criminal activity, but it is safe to assume cybercriminals make up a significant percentage of both bitcoin transactions and Tor usage. This mixture of untraceable web surfing combined with anonymous financial transactions became hugely appealing to criminal actors, and thus darknet markets were born.

[10] Roger Dingledine, Nick Mathewson and Paul Syverson, "Tor: The Second-Generation Onion Router," U.S. Naval Research Laboratory conference paper, 2004, *https://www.nrl.navy.mil/itd/chacs/dingledine-tor-second-generation-onion-router*.

[11] Blockchain, "Confirmed Transactions Per Day," accessed April 25, 2017, *https://blockchain.info/charts/n-transactions?timespan=all*.

Prior to 2014, many of the largest unauthorized exposures of data were caused by physical loss and theft of storage devices, laptops and paper files, as well as misconfigured servers and similar technical failures. Since that time, the number of sophisticated cyberattacks netting large numbers of records has risen significantly. Simultaneously, the rate of new malware creation and hacking tools such as advanced persistent threats (APTs), ransomware, spyware, malvertising and distributed denial of service (DDoS) attack tools have skyrocketed. This heightened activity among cybercriminals correlates with the rapid rise in bitcoin transactions (see Figure 1).

Figure 1. The Number of Daily Confirmed Bitcoin Transactions Since its Inception



Source: Blockchain, "Confirmed Transactions Per Day."

The rise in cybercrime is also due in part to the increasingly sophisticated business models employed by cybercriminals who enlisted computer engineers and software developers to create valuable cybercrime tools and a market for these wares among other cybercriminals. The next tier in this business model involves distribution infrastructure, which magnifies the spread of such cybercrime tools among a much larger and less skilled consumer base. A nontechnical cybercriminal can now buy time on a DDoS tool and launch an attack against a target anywhere in the world, via a point-and-click interface. Many of these services come with tech support. The same is true of multiple elements in the cyberattack process, where petty cybercriminals with minimal technical skill can gain access to sophisticated hacking tools and, for a small investment, use the tools to make a significant profit.

As mentioned earlier, the dominant currency of cybercrime transactions is bitcoin, though other cryptocurrencies are also used. Cryptocurrencies facilitated the rise of darknet markets (similar to an anonymous Amazon for criminals), where cybercriminals can set up shop to sell a wide range of illegal items including drugs, fake identity papers, weapons, stolen or grey market goods, stolen payment

card information, personally identifiable information, protected health information, federal tax information, sexual exploitation material and a wide array of criminal services. These markets include escrow services to provide some assurance that buyers and sellers actually deliver the goods and payments, as well as various metrics to ensure honor among cybercrooks, including reputation scoring and seller feedback. Some cybercriminals conduct transactions directly with counterparties and take advantage of the anonymous nature of communications via encrypted chat.

As noted earlier, cybercriminals seek to monetize all phases of the attack process, including intelligence gathered about potential targets. Many enterprises today contract with cyberthreat intelligence services that scan the dark web for mention of their organization, their products or profiles of their personnel as well as elements of their IT infrastructure. Such intelligence can be useful in determining the extent to which an organization has been targeted by cybercriminals. In some cases, threat intelligence turns up data or other indications that a compromise is in process or has already taken place.

Analysis of threat intelligence is also useful as a possible counterweight to the notion that "no cybercriminal would be interested in attacking our organization." This is a gross underestimation of cyberrisk in general and results from a poor understanding of cybercrime today. Cybercriminals continuously run automated scans of the entire internet, attempting to exploit any vulnerabilities they find, and infect vulnerable systems with malware, regardless of who owns it or what data it may contain. It is not uncommon for multiple intruders to infect the same vulnerable device. Such devices may be incorporated into a larger botnet (a collection of previously compromised computing systems that can be controlled remotely by a third party through a central command-and-control system) and used to assist in further criminal activities (like sending spam or scanning for vulnerable machines), or they may be encrypted and held for ransom. Sensitive data may be exfiltrated and sold, or the compromised machine may simply be warehoused for later use. Some current malware variants are capable of searching infected systems and networks for key words (such as hospital, bank, university) to determine what kind of target has been compromised and then it "phones home" to deliver the information to a command-and-control system. Cybercrime profit ratios have been estimated at 20:1 as the cost to the attackers for all this activity is negligible.[12]

Part 2. The Cyberrisk Ecosystem: Technological Evolution and the Rapid Rise of Cyberrisk

Over the past several decades, we have become increasingly reliant upon networked information systems in both our business and personal lives. This is true for our society as a whole, as nearly every area of our critical infrastructure depends on the proper functioning of information systems. The awe we may feel at the technological achievements of our digital ecosystem, and its seemingly magical capabilities, is diminished daily by the frequent, shocking headlines about successful cyberattacks and spectacular technical failures of systems. Although we would not have predicted these systems could be so vulnerable, upon closer inspection, a less awe-inspiring picture of our technological ecosystem

[12] Cisco, *Economics of Cybercrime: The Evolving Cybercriminal Business Model*, Cisco e-book, 2016.

quickly becomes apparent. This picture is neither new nor a well-kept secret.

In the physical world, rigorous inspections and certifications are an accepted part of the civil infrastructure design and construction process. In contrast, the cyberworld's infrastructure and software relies primarily on trust. Literally, a single key stroke, malicious or mindless, can hijack sensitive data from thousands of organizations. In 2015, defense contractor Lockheed Martin and the United Kingdom's Atomic Energy Authority were both attacked and lost highly sensitive data. Their systems were rerouted through unfriendly servers controlled by an ISP with ties to Russian organized crime for five days.[13] Similarly, in February 2017, a single mindless keystroke in a line of code caused private data, passwords, encryption keys and more to leak from thousands of websites and mobile apps into publicly searchable areas of the internet for months, while search engines around the world (including from China and Russia) cached the leaked data for future search and display.[14]

There are numerous quality assurance standards and security certifications for systems engineering and software development intended to prevent such mishaps. However, a study of secure software assurance by the United States Computer Emergency Readiness Team (US CERT) at Carnegie Mellon noted the recurring failure of software engineers to produce high-quality, secure software cost-effectively. Although software quality assurance standards are plentiful, they are not widely applied. According to US CERT, "But the real concern is that the exploitation of a software defect in a basic infrastructure component, like power or communication, could lead to a national tragedy like 9/11."[15] In the case of the 2015 traffic hijack, the border gateway protocol (BGP), which is used to route traffic around the internet, relies simply on trust between the parties who control the network equipment to enter the correct numbers and ensure appropriate routing of information around the world.

Software Makes the World Go Around (and Keeps Security Experts in Business)

Most consumers today want ubiquitous, "frictionless" interactions with the brands, products and services they like. Consumers of IT products have grown accustomed to the "patch Tuesday" approach to software development, which follows this sequence: build → deliver → fix → repeat. Of course, most developers incorporate some testing prior to delivery, but many developers lack the ability to do serious security testing. Many of the tools and frameworks employed by software developers do incorporate automated quality and security functions, but, as with all tools, the operator must be fully trained and appropriately incentivized to make effective use of such safeguards. As a result, this model has effectively turned software consumers into quality testers who pay for the privilege as well as the consequential costs of security vulnerabilities. Hence, the cost of cybersecurity losses is external to software and technology companies, rendering these organizations highly incentivized to get product

---

[13] Doug Madory, "UK Traffic Diverted Through Ukraine," Dyn's Research blog, March 13, 2015, *http://dyn.com/blog/uk-traffic-diverted-ukraine/*.

[14] "Cloudflare Reverse Proxies are Dumping Uninitialized Memory," reported by *taviso@goggle.com*, Feb. 19, 2017, *https://bugs.chromium.org/p/project-zero/issues/detail?id=1139.*

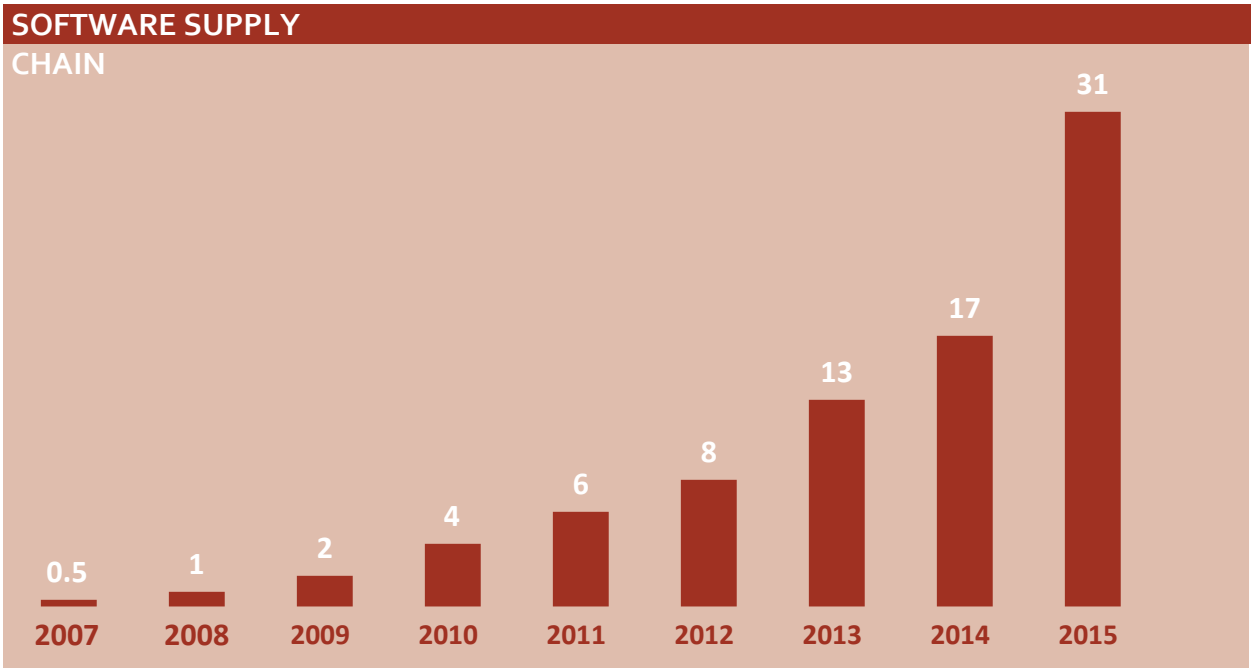
[15] Dan Shoemaker, Jeff Ingalsbe, Nancy Mead and Rita M. Barrios, "Defining the Discipline of Secure Software Assurance: Initial Findings from the National Software Assurance Repository," United States Computer Emergency Readiness Team (US-CERT) report, May 21, 2013, *https://www.us-cert.gov/bsi/articles/knowledge/software-assurance-education/defining-the-discipline-of-secure-software-assurance--initial-findings-from-the-national-software-assurance-repository*.

to market as quickly as possible, rather than to delay product release to ensure adequate security and quality control for consumers.

Cyberrisk and the Software Supply Chain

Commercial and in-house software development organizations have faced increasing pressure to reduce cost, streamline the software development process and speed software delivery. This has resulted in a paradigm shift away from writing software, toward a manufacturing model that entails building applications from reusable components and, in many cases, producing them off shore. Not unlike major automobile manufacturers, this model relies on an extensive software supply chain. A typical large enterprise software application supply chain includes several tiers of subsuppliers, contractors and vendors that provide thousands of software components. One open source component library called the Central Repository was accessed by over 10 million developers worldwide in 2015, and saw component downloads increase to 31 billion, up from 17 billion the prior year.[16] This is illustrated in Figure 2. Analysis of these downloads revealed that 6.1% had known security defects, a defect rate several orders of magnitude greater than typical automotive supply chains.

Figure 2. 31B Downloads by 10M Developers Worldwide from the Central Repository



Source: Weeks et al., "2016 State of the Software Supply Chain."

[16] Derek Weeks, et al., "2016 State of the Software Supply Chain," Sonatype report, *https://www.sonatype.com/software-supply-chain/*.

The Legion of the Bouncy Castle Cryptographic Library is one example that is particularly illustrative of the challenges inherent in this extensive use of software components. The Bouncy Castle software began in 2000 as a hobby project intended for use in securing software. In 2015, there were 17.4 million Bouncy Castle component downloads, of which 5.8 million (33%) were versions that contained known vulnerabilities. These defective components were downloaded by developers at 13,824 organizations in 197 countries.[17]

Web APIs: A Source of Revenue and Cyberrisk

This software supply chain combined with pervasive broadband internet access and cloud computing technology has engendered another digital ecosystem business model that is undergoing hypergrowth with important ramifications for cyberrisk. The web application programming interface (API) allows development organizations to quickly incorporate functionality from other web applications into their own, effectively providing direct, seamless integration and transactions with other enterprises. Developers can combine multiple APIs to create "mashups," such as a single travel booking webpage that contains functionality from Google Maps, Expedia travel bookings, Yahoo weather and Amazon product advertising, for example. The API economy has become big business. In 2015, Expedia generated 90% of its revenue through APIs, Salesforce.com generated 50% and eBay, 60%.[18] Even nontechnology companies like Walgreens have published APIs that developers have incorporated into new apps which allow consumers to print photos directly from their phones or social media accounts and pick them up at a local Walgreens.

The number of published APIs is rapidly growing, with one directory claiming to contain more than 50,000 APIs.[19] Web APIs are subject to the same defect rates and security vulnerability problems as other software products but with potentially more rapid and widespread impact. A recently discovered vulnerability in the WordPress API resulted in the defacing of thousands of websites within a matter of days. More than 18 million websites have WordPress installed, including 26% of the top 10,000 websites on the internet.[20]

Cyberrisk and Deperimeterization: Mobile, Cloud and the Untrusted Network

In recent years, internet access via mobile devices has steadily increased, globally surpassing desktop access as of October 2016. Some in the security community refer to this trend as "deperimeterization," a term that originated with the Jericho Group[21] more than a decade ago, and stemmed from the recognition that competitive enterprises require increased IT agility which extends beyond the network perimeter. Enterprises have been compelled to support more mobile and remote workforces, and

---

[17] Ibid.

[18] Bala Iyer and Mohan Subramaniam, "The Strategic Value of APIs," *Harvard Business Review*, Jan. 7, 2015, *https://hbr.org/2015/01/the-strategic-value-of-apis*.

[19] APIHound, API Directory Search, *http://apihound.com/apifinder*.

[20] Dave Lewis, "Wordpress 0-Day Content Injection Vulnerability," *Brick of Enlightenment* (blog), Feb. 1, 2017, *http://www.csoonline.com/article/3163629/security/wordpress-0-day-content-injection-vulnerability.html*.

[21] Jericho Forum, "Architecture for De-perimeterisation" position paper, version 1.0, April 2006, *https://collaboration.opengroup.org/jericho/Architecture_v1.0.pdf*.

provide their customers with broad access to their brand, products and services. Deperimeterization therefore recognizes the vital significance that information architecture must be re-designed to support secure operations on untrusted networks. Innovations in mobile and cloud technology have so successfully reduced costs and increased performance that a productive, cost-effective, remote and mobile workforce is commonplace today. However, the challenge of preventing nefarious actors from accessing enterprise applications and sensitive data, whether from outside the traditional network perimeter or from within, has grown increasingly more difficult. As mobile, cloud and remote access technologies have become more prevalent, so have the sophisticated attacks against them.

Uptick in Mobile Malware Attacks

Nokia analyzed data from more than 100 million devices and found the average monthly infection rate among smartphones increased 98% in the first half of 2016 compared to the same period in 2015.[22] The security vendor Intel/McAfee reported a new record was set during the same period, with more than 2 million new mobile malware samples recorded, reflecting 151% growth over the previous year.[23] Despite the uptick in malware attacks against smartphones, Android-device manufacturers issue far fewer, averaging only 1.26 security updates per year,[24] unlike Microsoft, which issues security patches to PCs on the second Tuesday of each month.

Remote workers using small office/home office (SOHO) networking equipment have not escaped the tentacles of cybercriminals either. Millions of vulnerable home routers have been exploited globally over the past several years and incorporated into botnets, which have, in turn, been used to launch cyberattacks. In addition to presenting security risk to home offices and individuals, these and millions of other internet-connected devices have been used to launch unprecedented attacks against specific targets. One such attack against internet infrastructure service provider Dyn occurred in October 2016 and, for a day, blocked access from major portions of the internet to hundreds of major websites including Netflix, Twitter and CNN[25]. A similar attack in November 2016 exploited weaknesses in routers and caused 900,000 Deutsche Telekom users to lose internet access.[26] Other attacks against home offices and mobile users redirect traffic to malicious sites, compromise devices on the network, and decrypt and exfiltrate data. Some mobile malware variants have enlisted compromised Android devices to attack home routers.

---

[22] Nokia, "Nokia Threat Intelligence Report—H1 2016," 2017, *https://resources.ext.nokia.com/asset/200492*.

[23] McAfee, "McAfee Labs Threats Report, September 2016," *https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf*.

[24] Daniel R. Thomas, Alastair R. Bersford and Andrew Rice, "Security Metrics for the Android Ecosystem," paper, October 2015, *https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf*.

[25] Nicky Woolf, "DDoS Attack That Disrupted Internet was Largest of its Kind in History, Experts Say," *The Guardian*, Oct. 26, 2016, *https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet*.

[26] Dan Godin, "Newly Discovered Router Flaw Being Hammered by In-the-Wild Attacks," Ars Technica's Risk Assessment blog, Nov. 28, 2016, *https://arstechnica.com/security/2016/11/notorious-iot-botnetsweaponize-new-flaw-found-in-millions-of-home-routers/*.

Breaches in the Cloud

Several breaches have occurred at high-profile, cloud-based service companies such as Yahoo and LinkedIn, making major headlines last year because of the security issues themselves and because both companies grossly underreported the gravity of the monumental breaches. LinkedIn's breach grew 18 times from the 6.5 million accounts originally reported to 117 million[27]. Yahoo announced an initial breach of 500,000 accounts and followed up two months later with the announcement of another separate breach of a billion accounts[28]. (If you have accounts with either of these two services and haven't changed your passwords yet, it's still better to do so late than not at all!)

Over the past three years, billions of records containing personally identifiable information (PII) and protected health information (PHI) have been stolen from cloud-based services. Such incidents continue to make headlines on a regular basis. A recent study based on data from 30 million users at enterprises around the world revealed that cloud-related threat incidents increased 18.4% over the prior year, to an average of 23.2 incidents per month.[29] These included insider threats (both malicious and accidental) as well as compromised accounts and exfiltration of sensitive data. From an enterprise risk management point of view, however, it is important to note the term "cloud" covers a wide range of internet-based technologies. These typically include: outsourced data-center resources like Infrastructure as a Service (IaaS), internet-based development environments known as Platform as a Service (PaaS) and, perhaps the most familiar, Software as a Service (SaaS), which provides access to cloud-based applications and database services. In addition, many mobile applications connect to internet-based Backend as a Service (BaaS), which have also experienced massive, high-profile compromises.

One thing all of these cloud services have in common is the ease with which they can be provisioned and accessed. Anyone with internet access and a credit card can set up an account and launch servers with fully functional applications in a matter of minutes. Enterprises that conduct cloud audits find that their IT departments underestimate cloud usage within their organization by a factor of 10.[30] This phenomenon, commonly referred to as "shadow IT," provides a good indication of how this type of cyberrisk bleeds into several other areas, including legal and compliance, governance, vendor and supply chain management, business continuity, insurance and risk transfer.

How to Manage What You Can't Measure

No risk manager would disagree with the statement that managing cyberrisk is challenging. Cyberrisk is complex, dynamic, and undergoing continuous and rapid change. Cybersecurity is an asymmetric game to the

---

[27] Dan Godin, "LinkedIn Says Hacking Suspect is Tied to Breach That Stole 117M Passwords," Ars Technica's Policy blog, Oct. 19, 2016, *https://arstechnica.com/tech-policy/2016/10/linkedin-says-hacking-suspect-is-tied-to-breach-that-stole-117m-passwords/*.

[28] Lily Hay Newman, "Hack Brief: Hackers Breach a Billion Yahoo Accounts. A Billion," *Wired*, Dec. 14, 2016, *https://www.wired.com/2016/12/yahoo-hack-billion-users/*.

[29] Skyhigh Networks, "Cloud Adoption Risk Report, Q4 2016," *http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-and-Risk-Report-Q4-2016.pdf*.

[30] Skyhigh Networks, "Cloud Adoption and Risk in Financial Services Report, Q2 2015," *http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-and-Risk-In-Finance-Q2-2015.pdf*.

distinct disadvantage of the defender. Intelligent adversaries continue to innovate, respond to and actively evade mitigation efforts. Cybercriminals have few time constraints when designing an attack, but the timeframe for responding to new cyberthreats and vulnerabilities is measured in minutes, hours and days. Risk managers must also contend with cyberrisks that extend beyond such malicious actors to include the innocent mistakes of insiders, vendor outages, system failures, architectural flaws and environmental hazards.

Few organizations today have the means to invest in establishing quantitative cyberrisk measures that remain meaningful long enough to deliver an acceptable return on investment, especially considering that the financial impact of cyberloss events have not been as large as many other categories of operational risk. This is compounded by the fact that much of the hype, and the dire predictions regarding breach costs, customer churn and stock market losses along with consequential damages to brand and reputation have not been borne out by reality. Given these facts, we are justified in posing the obvious question: Why spend so much money and attention on cyberrisk? Perhaps the answer lies in our intuition that although we have yet to experience a truly catastrophic cyberevent, the high frequency of less severe incidents has demonstrated just how vulnerable we are. It doesn't take much imagination to conceive of the costs such an event could exact on an individual enterprise or our society.

Despite the widespread acceptance of this intuition, the challenges of measuring cyberrisk are compounded by the fact there is little consensus among experts on how to measure cyberrisk, or even which cybersecurity metrics are most relevant or useful. Experts in the field (professional and academic) have not even established a single, widely accepted set of definitions for key cyberrisk terms (including "cybersecurity"). Although many organizations have begun to collect and analyze internal data about cyber-related incidents, there is very little reliable external cyber incident or loss data available that contains sufficient detail to establish benchmarks, data validation or external comparisons. Without such loss data, clear metrics or a standardized framework, the creation of a reliable, generalizable mathematical cyberrisk model and the assignment of confidence levels to cyberrisk forecasts for an individual organization remains an unconquered summit.

This is not to say there is no way to assess cyberrisk. One can find several companies that conduct a range of useful cyberrisk assessments, and some companies sell generalized cyberrisk scoring services. Most often, however, measures of cyberrisk are presented to senior management in the form of a heat map that displays qualitative assessments of risk, prioritized in a quasi-mathematical picture.

What Can Risk Managers Do?

Despite these quantification challenges, there are some definitive steps risk managers can take to advance the state of communication and understanding regarding management decisions around cyberrisk. A first step is to examine the ways your organization fits into the broader cyberrisk ecosystem. It may at first seem counterintuitive to extend the scope of cyber risk management to an even broader, multidimensional "ecosystem" that extends up to the cloud, down to the dark web and around through the world of mobile devices, back through the supply chain and forward to the Internet of Things, while at the same time acknowledging the inadequacy of our current efforts to measure and manage the risk posed by our internal systems, processes and people. Nonetheless, this is, in fact, in keeping both with

the state of cyberrisk and of operational risk management. Operational risk management includes addressing the risk of loss from external factors and events, and as noted, cyberrisk has largely been deperimeterized. Insights about these external factors can inform and improve internal processes, and shed a brighter light on the systemic impacts that will allow for more risk-aware decisions.

As noted, the cyberrisk ecosystem extends well beyond the systems under IT's control, and in many cases, an organization's critical risks stem from these nonobvious sources.[31] The discussion of the cyberrisk ecosystem in Part 1 of this paper presented several examples of significant and continuous contributors to cyberrisk commonly found in enterprises today. Identifying any of these and other applicable elements within the broader cyberrisk ecosystem can help an enterprise map the interrelationships among them, and possibly reveal some of the root causes underlying the experience of cyberrisk across the enterprise. Without such analysis, cyber risk management will continually struggle to keep these experiences from reoccurring.

As consumers come to expect more ubiquitous, "frictionless" experiences, the push to rapidly deploy integrated mobile and cloud-based systems to remain competitive will likely continue unabated. While this combination represents a significant expansion of the attack surface to cybercriminals, organizations that develop a deep understanding of the governance, security and cyber risk management ramifications across the enterprise will be in a much better position to turn the management of these risks into a competitive advantage.

Part 3. Cyber Insurance and Emerging Correlated Risks

Cyber insurance plays a critical role for enterprise cyber risk management. The number of organizations that depend on cyber insurance to manage the risk of high severity events has been rapidly growing over the past several years. The market has matured and carriers have gained a better understanding of the risks as well as the exclusions and sublimits that make sense but are still acceptable to the marketplace. Despite a small number of high-profile cyberlosses, the market for cyber insurance has exhibited steady growth with some of the leading carriers experiencing 100% growth in gross written premium year over year.[32] Although the insurance industry is traditionally known for stability and reliability rather than agility, the ability of carriers in this market to respond to the dynamically changing cyberthreats facing their customers may prove to be the defining competitive edge.

---

[31] The ecosystem includes a multi-tiered software supply chain with vendors several steps down the chain embedding critical components into the organization's operating environment. The ecosystem includes business partners, sharing and receiving information, and critical functionality through APIs. The ecosystem includes mobile and cloud-based products and services, which may be provisioned at multiple points throughout the organization. The ecosystem includes the bottom feeders behind the attacks, those malicious actors inhabiting the depths of the dark web who seek out and take advantage of weaknesses at all levels of the organization. The ecosystem also includes the internet-connected sensors, processors and actuators that make up the Internet of Things, along with the next technological innovation just appearing on the horizon.

[32] Richard Betterly, "Cyber/Privacy Insurance Market Survey: 2016," The Betterly Report (June 2016), *https://www.irmi.com/docs/default-source/authoritative-reports/betterley-executive-summaries/cyber-privacy-media-liability-summary-2016.pdf*.

Like other risk managers, cyber insurers struggle to employ reliable, quantitative evaluation of cyberrisk. In addition, individual insureds tend to renew year after year, without necessarily undergoing a thorough underwriting process after each change in their IT infrastructure or business model. As noted above, these changes may cause significant alterations in the cyberrisk exposure of an organization and yet remain completely under the radar of the carrier. Cyber insurance carriers and their reinsurers are subject to aggregated, systemic losses. Four examples follow of how single points of failure in the cyberrisk ecosystem can impact large portions of a carrier's book of business as well as its reinsurer's portfolio. Three of these events occurred in the same month.

Two Software Flaws, 22 Million Websites

Two incidents involving software flaws demonstrate the potential for a single cyberincident to affect a large number of independently insured entities. One such event described briefly at the start of this paper occurred in late February 2017 and involved a programming defect in a line of code at internet infrastructure provider Cloudflare that caused the accidental leakage of sensitive information. Cloudflare operates a content delivery network (CDN) that hosts some 4.2 million domains as well as major smartphone apps including Uber, Fitbit, Dropbox and Microsoft Outlook.[33] Although the number of entities actually reporting unauthorized disclosures in the near term following this event is likely to be small, the leaked data has been cached by search engines around the world and will quite possibly remain searchable in places like Russia and China for a long time. Cloudflare claimed that only .00003% of pages contained the leaked data but, given the enormous scale of Cloudflare's operation, that still amounts to between 100,000 and 200,000 pages per day.[34]

Another software defect discovered in February with serious security ramifications was the WordPress API bug. The bug was exploited by malicious actors and 1.5 million websites were defaced within three weeks.[35] WordPress is installed on approximately 18 million websites around the world including 26% of the top 1,000 most popular websites, according to website ranking company, Alexa. No cost estimate for the losses has been publicized.

The third example during the same month involved an outage at Amazon's S3 (Simple Storage Service) and related infrastructure in its U.S. East facility in Virginia that lasted about four hours with even longer impacts to many of its customers. Amazon explained the outage was caused by an authorized engineer who made a mistake in executing a maintenance procedure. By taking down storage required by other Amazon systems, the error caused a cascading failure that impacted several critical Amazon services. Amazon's dominant position in the cloud hosting and infrastructure service industry means the outage impacted thousands of organizations such as the U.S. federal government, Google, Apple, Uber and

---

[33] Michael Mimoso, "Cloudflare Bug Leaks Sensitive Data," Threat Post's Privacy blog, Feb. 24, 2017, *https://threatpost.com/cloudflare-bug-leaks-sensitive-data/123891/*.

[34] "List of Sites on Cloudflare DNS (archived)," GitHub.com, accessed April 25, 2017, *https://github.com/pirate/sites-using-cloudflare*.

[35] Chris Brook, "1.5M Unpatched Wordpress Sites Hacked Following Vulnerability Disclosure," Threat Post's Vulnerabilities blog, Feb. 10, 2017, *https://threatpost.com/1-5m-unpatched-wordpress-sites-hacked-following-vulnerability-disclosure/123691/*.

numerous internet retailers, financial institutions and much of the Fortune 500. The loss to Amazon S3 customers caused by this four-hour outage was estimated at about $310 million.[36]

The fourth example, which occurred in October 2016, was the attack against Dyn, an internet infrastructure provider. Dyn was the victim of the largest DDoS attack in the history of the internet up to that point in time. Consumers from both the east and west coasts of the United States, as well as parts of Europe, Asia, Africa and South America were unable to access hundreds of major websites for most of the day. Even though Dyn does not actually host the websites, this outage effectively knocked these sites off the internet. Dyn is responsible for hosting domain name services (DNS), part of the critical infrastructure of the internet. It is estimated the attack cost about $100 million in losses to the impacted customers. It is also estimated Dyn lost some 14,500 hosted domains following the attack.[37]

The attack against Dyn was launched from a botnet consisting of about 100,000 compromised Internet of Things devices. Rather than monetize the code behind this exceptionally powerful botnet (called Mirai), the author released the code into the wild on the dark web and other attackers have since deployed it, and a closely related variant, against different targets to devastating effect. Many of the compromised devices used in the Dyn attack are low-cost, internet-connected consumer video cameras, baby monitors, routers and other IoT items that in many cases were not designed to be updated or patched. The Mirai botnet is an example of one highly powerful weapon cybercriminals have at their disposal that is likely to attract others to develop variants and which will continue to grow more and more dangerous as time goes on. It also reflects the asymmetry in the cyberrisk ecosystem that favors the offense over the defense.

The number of connected devices on the Internet of Things is projected to reach 30 billion to 50 billion by 2020. Given the economics of the lower-end IoT devices, it is unlikely these devices, or the millions of others containing serious vulnerabilities, will ever be fixed without some kind of regulatory requirement. The ever-expanding supply of such "unfixable" IoT devices still being produced and connected to the internet is just waiting to be compromised and repurposed into larger and larger DDoS weapons. Unskilled cybercriminals (or even just an angry teen, as is suspected in the Dyn attack) can employ these weapons to target internet infrastructure or other systems, potentially causing significant losses to large numbers of entities in both the cyber and the physical worlds.

In Closing

In this paper, some of the recent shifts in information technology that have had direct, far-reaching impacts on the cyberrisk ecosystem have been described. As defined in this paper, the cyberrisk ecosystem includes networks of interrelated actors and systems that operate on both the surface web

[36] Trevor Jones, "Amazon S3 Outage Spotlights Disaster Recovery Tradeoffs," SearchAWS.com TechTarget, March 2, 2017, *http://searchaws.techtarget.com/news/450414316/Amazon-S3-outage-spotlights-disaster-recovery-tradeoffs?utm_medium=EM&asrc=EM_NLN_73757925&utm_campaign=20170307_AWS%20downtime%20highlights%20users%27%20redundancy%20limits&utm_source=NLN&track=NL-1814&ad=913167&src=913167*.

[37] Adrienne LaFrance, "How Much Will Today's Internet Outage Cost?" *The Atlantic,* Oct. 21, 2016, *https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/*.

and the dark web. As we go about our daily digital activities, the darker side of the cyberrisk ecosystem is not obvious to most of us. Nonetheless, the surface web and the dark web are interconnected. Both are driven by related technological, economic and social forces, many of which are capable of producing both social benefits and costs. Cryptographic technology, for example, has enabled privacy and authentication functions essential to the world of digital transactions and communications on the surface web but has also played a critical role in enabling anonymity in criminal transaction.

One major point of divergence can be seen when the ecosystem is viewed through the lens of risk. Actions taken, and actions deferred, by technology organizations as well as consumers have led to massive flows of value moving in one direction—from the surface web to the dark web. This fact, along with the recognition that internet computing has reached a scale where massively aggregated risk is the norm, provide strong motivation for risk managers and insurers to explore new ideas and new methods of managing cyberrisk.

In spite of the cybersecurity challenges presented by IoT devices, Hartford Steam Boiler (HSB), a member of Munich Re's Risk Solutions group, has begun to explore new approaches to managing cyberrisk. As its name suggests, Hartford Steam Boiler started out insuring industrial equipment more than 150 years ago. The Internet of Things consists of sensors that gather information about the environment and processes, processors which process that information, and actuators which move things and make changes in the physical world. The IoT may be new, but this is very familiar territory for HSB. This may help explain why this venerable insurance company is trying such an innovative approach to cyber risk management with the launch of an IoT insurance product in conjunction with IoT technology solutions provider relayr. Another explanation may be found in the fact that the industrial IoT (IIoT) market is projected to grow to $225 billion by 2020, one third larger than the $170 billion projected for the consumer IoT.

The collaboration between an IoT technology company and an insurance company pairs cyberrisk mitigation with cyberrisk transfer in a way that may lead to innovative solutions providing enhanced protection to both organizations and consumers. Munich Re/HSB Ventures is also leading a financing round for relayr. It is not unlikely that such collaborations will become more common in the world of cyberrisk, as a tighter integration between cyberrisk mitigation and cyberrisk transfer may result in more than the sum of its parts.