CSX™
CYBERSECURITY NEXUS

Cybercrime: Defending Your Enterprise

How to Protect Your Organization From Emerging Cyberthreats

Abstract

Over the last 25 years, cybercrime silently evolved from an abstract idea into a tangible threat to the global marketplace and security sector. The sharp increase of Internet-based attacks over the last five years has resulted in nation-states, enterprises, media and cyber security experts openly discussing this dire problem. Ineffective coordination of public and private entities to affect positive change toward the common goal of Internet protection across the world increasingly emboldens cybercriminals. This ineffective coordination manifests itself in a lack of incident data sharing and cooperation, and incompatible laws and regulations to mitigate nefarious activities in the digital space. Despite the infancy of global cooperation to defend against emerging global cyberthreats, an enterprise can establish measures to better protect itself. This whitepaper helps you to gain a better understanding of some of the more prominent emerging cyberthreats and arms you with measures to defend your enterprise from these threats.

ISACA®
Trust in, and value from, information systems

Table of Contents

Cybercrime

Cybercrime costs the global economy an estimated $445 billion per year, according to a 2014 report by the security firm McAfee Labs.[1] As the 21st century advances, rapid technological evolution continues to establish an interconnected world of online enterprise and personal activity, increasing the threat to our global economy and security. Cybercrime, defined as criminal activity that is committed or facilitated via the Internet, continues to grow along with the number of global Internet users.[2, 3, 4] The increased convenience and interconnectivity of the Internet that is encouraging entire enterprises to move their business, data and financial resources to the digital domain is multiplying cybercrime opportunities, while decreasing the risk of exposure for criminals. The movement of money onto the digital domain attracts enterprising criminals, resulting in greater criminal activity worldwide.[5] Criminals leverage sophisticated tools to target and attack millions of people and enterprises online. Ineffective coordination of Internet protection, minimal incident data sharing and incompatible international laws and regulations further embolden nefarious actors in the digital space. However, applicable security measures to protect enterprise assets are being created, with the help of analyses of current attacks and emerging target vectors.

A Survey of Attacks

Comprehension of the cybercrime threat requires a cursory analysis of its effects on today's industry. Since 2010, online criminal activity continues to explode. Juniper Research estimates the cost of cybercrime will climb to an estimated US $2.1 trillion by 2019,[6] far exceeding the revenue generated by more traditional criminal activity, such as the drug trade (estimated at US $600 billion).[7] Certain high-profile hacking incidents involve targeting of personally identifiable information (PII). Collectively, cyberattackers stole approximately 100 million records, including names, Social Security numbers, financial information and dates of birth, during attacks on UCLA Health, Premera Blue Cross Blue Shield and Anthem. Criminals also target retailers and online forums to gain access to PII. Approximately 15 million T-Mobile customers were compromised when a third-party vendor (credit company Experian) was attacked in September 2015. Experian lost credit check-related information of T-Mobile customers, including passport information.[8] 37 million PII records that were stolen during the Ashley Madison website breach resulted in a dump of PII on public-facing websites for the purpose of humiliation.[9, 10] In 2014, the Singapore K Box Entertainment Group had over 300,000 customer records stolen.[11] In India, according to a 2015 KPMG report, the number of cyberincidents has risen with a trend toward financial cybercrime. KPMG respondents

1 McAfee, Inc., "Net Losses: Estimating the Global Cost of Cybercrime," 2014, *www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf*

2 National Crime Prevention Council, "Cybercrimes," 2012, *www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf*

3 INTERPOL, "Cybercrime," 2016, *www.interpol.int/Crime-areas/Cybercrime/Cybercrime*

4 European Commission, "Cybercrime," 4 February 2015, *http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm*

5 McAfee, Inc. "McAfee Labs Threats Report," August 2015, *www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf*

6 Juniper Research, "Cybercrime Will Cost Businesses Over $2 Trillion by 2019, Finds Juniper Research," PR Newswire, 12 May 2015, *www.prnewswire.com/news-releases/cybercrime-will-cost-businesses-over-2-trillion-by-2019-finds-juniper-research-503449791.html*

7 Lewis, James; The Economic Impact of Cybercrime and Espionage, The Center for Strategic and International Studies (CSIS) and McAfee, 2013, *www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf*

8 ZDNet, "These Companies Lost Your Data in 2015 Biggest Hacks, Breaches," 30 November 2015, *www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2015/2/*

9 *Ibid.*

10 Baraniuk, Chris, "Ashley Madison: 'Suicides' over website hack," BBC News, 24 August 2015, *www.bbc.com/news/technology-34044506*

11 Singapore Press Holdings Ltd. Co., "Personal data of 300,000 K Box Singapore clients surfaces online," SPH Digital News, 16 September 2014, *www.straitstimes.com/singapore/personal-data-of-300000-k-box-singapore-clients-surfaces-online*

indicated that 63 percent of their enterprises suffered financial loss due to cybercrime.[12] Cybercriminals also regularly launch attacks against enterprises across Europe where Germany, the second biggest victim of cybercrime, experiences attacks against the financial, energy and pharmaceutical sectors.[13] With no end in sight, Ernst and Young declared cybercrime the greatest global threat to enterprise survival today.[14]

Current and Emerging Methods

Although criminals adopt their tactics based on evolution of the Internet ecosystem, they also continue to use many tried and true cybercrime methodologies. For example, social engineering continues to be the most-used attack methodology.[15] This white paper focuses on the following cybercrime activities for 2016 and beyond:

- Extortion—Holding enterprise data for ransom
- Dark cloud use—Leveraging cloud services for cybercrime
- Appliance attacks—Targeting the increasing surfaces of the Internet of Things (IoT)

Extortion—Held at Ransom

Cyberextortion is an attack or threat of attack that is tied to a demand for money to prevent or stop the attack. Extortion involves cybercriminals implementing ransomware that encrypts data on a victim's system. Victims of ransomware typically receive a notification email soon after their system is locked, offering a private decryption key in exchange for a monetary digital currency payment, such as Bitcoin. Often, enterprises and individuals pay the ransom, finding it cheaper and timelier than trying to break the encryption. Although payment of the ransom does not always guarantee the provision of the decryption key, a growing trend indicates that cybercriminals provide the key to maintain a reputation for keeping their promises. In a November 2015 InfoWorld article, senior security advisor Chester Wisniewski confirms that whether ransom is paid is often determined by the attacker's reputation. Wisniewski gives the example of CryptoWall ransomware. The criminals behind CryptoWall show a desire to keep a good brand name and customer reputation by consistently decrypting files when they receive ransom payment. In addition, they provided time extensions for victims to obtain the ransom money. Abiding by their word is good business; however, not every criminal enterprise can be trusted to decrypt files after receiving ransom payment.[16]

Preventing Cyberextortion

With the looming expectation that cyberextortion will grow over the next five years, recommended strategies include the following:

- Know what constitutes your enterprise data—understand the data that you own and what is at risk.
- Back up enterprise data—then back it up again. Create data backups regularly.
- Conduct re-occurring security awareness training—implement brief quarterly blocks of training that focus on preventing phishing, waterholing and other social engineering attacks.
- Restrict network access according to the principle of least privilege—ensure that administrators and employees only have access and privileges on the network that are necessary for them to perform their jobs.
- Employ the appropriate technical tools to mitigate intrusions—ensure the use of robust firewalls, intrusion detection systems, end-point protection and anti-virus technology.
- Evaluate security settings of web browsers and email software to ensure that they provide an appropriate level of security to meet business requirements (e.g., auto scanning of all attachments and whitelisting websites).

12 KPMG, "Cyber Crime Survey Report: India," November 2015, *www.kpmg.com/in/en/issuesandinsights/articlespublications/pages/cyber-crime-survey-2015-30nov15.aspx*

13 Ponemon Institute, "2015 Cost of Cybercrime Study: Global," October 2015, *https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*

14 Ernst & Young, "Cyber-crime is greatest global threat to organizations' survival today," 29 Oct 2013, *www.ey.com/GL/en/Newsroom/News-releases/News_Cyber-crime-is-greatest-global-threat-to-organizations-survival-today*

15 ISACA and RSA Conference, "State of Cybersecurity: Implications for 2016," 2016, *www.isaca.org/cyber/Pages/state-of-cybersecurity-implications-for-2016.aspx*

16 Rashid, Fahmida Y., "Facing cyber blackmail? Don't pay a king's ransom," InfoWorld, 16 November 2016, *www.infoworld.com/article/3003384/security/facing-cyber-blackmail-dont-pay-a-kings-ransom.html?utm_source=tuicool&utm_medium=referral*

- Update software patches regularly—patch on a regular, organizationally defined basis.
- Apply distributed denial of service (DDoS) armor—invest in DDoS attack protection to be able to absorb DDoS attacks without significant system degradation.
- Develop and exercise the enterprise incident response plan—create a plan and exercise it regularly across all departments to ensure effective communication and maintain basic continuity of operations.

Dark Clouds—Crime Moves From the Enterprise and Individual to the Cloud

According to "The Global State of Information Security Survey 2016," from PwC, nearly 70 percent of respondents state that their enterprises use cloud-based cybersecurity services.[17] Across the globe, enterprises continue to migrate to the cloud in record numbers to take advantage of the flexibility, cost savings, and massive access to storage and computing power. Although cloud service providers are touting the business advantages and security of cloud migration, cybercriminals view it subversively. The cloud provides cybercriminals with the same advantages that legitimate enterprises enjoy, but with subversive goals. Criminal enterprises in the cloud complicate detection. Their attacks access global systems and provide a base from which cybercriminals can control operations, mount attacks on connected systems and even steal space to store stolen data.

Once breached, a cloud environment offers access to vast amounts of information that can be repurposed for the criminal profit-making enterprises. These cybercrime enterprises are able to leverage stored personal customer information, financial data, intellectual property, policy, business strategy and emerging research for their own profit. For example, in May 2014, Trend Micro researchers discovered cybercriminals using Dropbox® to carry out malicious command-and-control operations. This methodology demonstrates that cybercriminals are no longer satisfied with merely hosting and launching malware within the cloud; they are now managing their attacks remotely. The cybercriminals ensure that communication between the command-and-control software and the malware sites looks like normal network traffic.[18] Cybercriminals are leveraging cloud services, like legitimate enterprises, to simplify implementation and reduce costs.

Protecting the Cloud

As enterprises continue to migrate to the cloud, criminals follow. Cloud protection is a joint effort between the enterprise and the cloud service provider. To protect against unauthorized cloud access, enterprises must establish right of audit agreements with service providers and apply many of the same measures that protect them from extortion, including the following:

- Patch systems, browsers and applications.
- Apply antivirus and anti-malware tools.
- Install firewalls and intrusion detection systems.

The cloud service providers must apply the following protections:

- Implement multifactor authentication to strengthen authentication checks.
- Encrypt data that travels between the cloud and the customer.
- Encrypt data that are stored in the cloud.
- Patch systems, browsers and applications.
- Apply antivirus and anti-malware tools.
- Install firewalls and intrusion detection systems.
- Inhibit physical access by criminals through preventive and detective measures, such as alarms, fences, cameras and biometric access.
- Provide attestation reporting on the effectiveness of internal controls to clients.

Service level agreements must be well understood by the enterprise and the cloud service provider; must address security, privacy and data control issues; and must set third-party audit requirements of cloud service providers.

17 PwC, "The Global State of Information Security® Survey 2016," 2016, *www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html*

18 Menrige, Maersk, "PlugX RAT With 'Time Bomb' Abuses Dropbox for Command-and Control Settings," Trend Micro Incorporated, 25 June 2014, *http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/*

Appliance Attacks—Assaults on Things

As devices become more interconnected, creating the IoT, they provide additional opportunities for cybercriminals. Attacks include raising or lowering the thermostat and shutting off or causing appliances to malfunction (e.g., turning off refrigerators and bypassing water heater temperature restrictions). Although most of these attacks may not put a person's life at risk, physical harm is possible because IoT components rely heavily on unmonitored firmware or basic operating systems. Some firmware requires a connection to the Internet to work properly or enable additional features. These connections are susceptible to hackers/cybercriminals who leverage a connection to remotely control a device. In 2014, the security firm Proofpoint discovered a botnet attack leveraging televisions, home multimedia devices, routers and even a refrigerator to send 750,000 spam emails, three times a day.[19] Tracing attacks may become increasingly more difficult with the explosion of the attack surface. According to Juniper Research, by 2020, the number of connected devices will reach 38.5 billion, which is a 285 percent increase over the 13.4 billion Internet-connected devices in 2015.[20]

Wireless medical technology is another serious IoT target. Technology-enabled devices are integrated into the human anatomy for various reasons and include pacemakers, insulin pumps and devices for basic health monitoring. Embedded biotechnology can hold almost all personal data, track individuals, and enable biometric interaction between man and machine. This technology can be targeted wirelessly, because it often relies on radio-frequency identification (RFID) or Bluetooth® technology. Embedded biotechnology, such as an implanted near-field communications chip (NFC), permits health care providers to collect valuable data or control the rhythm of a heart, but many have no built-in security, such as encryption or protective hardware or software. Additionally, many of these biotechnology devices cannot receive a firmware update. After they are embedded in the body, surgery is required to update them. Researchers at MacAfee demonstrated that a pacemaker can be remotely hacked to deliver an 830-volt shock to the heart from more than 50 feet away.[21]

Stopping Assaults on Things

The increasing volume of devices that are emerging with IP addresses for network connectivity creates a massive problem set for enterprises and individuals to secure from cybercriminal attack. Based on reported breaches originating from Internet-connected devices, enterprises saw a 152 percent jump in attacks in 2015.[22] As criminal activity targeting IoT devices continues to escalate, enterprises must take steps to protect their networks of devices. Recent recommendations from cyber security experts and law enforcement include:[23, 24]

- Use perimeter protections, including an intrusion prevention system and a firewall.
- Employ a security information and event management (SIEM) system.
- Integrate an identity access management central user control program into your IoT devices.
- Implement multifactor authentication in practical situations.
- Enforce privileged user account controls for all administrators.
- Research and employ industry-standard best practices and security controls already developed for existing architecture, such as those found in National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) documentation.
- Consider due diligence for third-party IoT providers.
- Isolate IoT devices on their own protected networks (e.g., guest network).

19 Starr, Michelle, "Fridge Caught Sending Spam Emails in Botnet Attack," CNET, 19 January 2014, *www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/*

20 Juniper Research Ltd, "'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020," 28 July 2016, *www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020*

21 Wadhwa, Tarun, "Yes, You Can Hack A Pacemaker (And Other Medical Devices Too)," Forbes, 6 December 2012, *www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/#40c03bde13e0*

22 Sci-Tech, "Internet of Things: Cyber Crime on the Rise," 2 February 2016, *www.euronews.com/2016/02/02/internet-of-things-cyber-crime-on-the-rise/*

23 Poremba, Sue; "How Smart Devices Let Cybercriminals into Your Home," Risk Sense, 2016, *www.risksense.com/how-smart-devices-let-cybercriminals-into-your-home/#.VyBf6mdwUiS*

24 Paganini, Pierluigi, "A Recent Announcement Issued by the Federal Bureau of Investigation Warns Customers that Internet of Things Poses Opportunities for Cyber Crime," Security Affairs, 15 September 2015, *http://securityaffairs.co/wordpress/40139/cyber-crime/fbi-internet-of-things.html*

- Review the intended purpose and the necessity of IoT devices.
- Use a proven supply chain for device purchasing.
- Patch IoT devices as soon as it is practical.
- Understand device capability and how appliances use wireless connectivity—change default passwords, encrypt Wi-Fi connections, ensure the device only operates on designated networks.
- Change all default passwords to strong passwords. Avoid using a device-manufactured default password. This is a sound best practice, because many default passwords can be easily located on the Internet.

Conclusion

Enterprises will continue leveraging the capabilities provided by the Internet to establish streamlined processes and keep current in the competitive business world. However, it is important to understand that, similar to these enterprises, criminals also utilize new capabilities as they emerge. By implementing the steps provided in this white paper, enterprises can create a robust security posture to better protect themselves from cybercrime.

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances. ISACA nor this publication is associated with or sponsored by Amazon Technologies, Inc.

Reservation of Rights

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

www.isaca.org

Provide feedback:
www.isaca.org

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
www.twitter.com/ISACANews

Join ISACA on LinkedIn:
www.linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ACKNOWLEDGMENTS

ISACA would like to recognize:

Lead Developer

T. Frank Downs
CEH, ECSA, LPT, CEI, ISACA, USA

Expert Reviewers

Josh Angichiodo
Lieutenant Commander, US Navy

Keith Brown
CISA, CISSP, SunTrust, USA

Michael Marano
CEH, CWTS, CWNA, CWNP, CEI, OSWP, INNOPLEX, LLC, USA

ISACA Board of Directors

Christos K. Dimitriadis Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Greece, International Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, US House of Representatives, USA, Vice-chair

Robert Clyde
CISM Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Director

Jo Stewart-Rattray CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management Inc., USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research, USA, Past ChairCyberc

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT FASAE, CAE, ISACA, USA, Director

Cybersecurity Working Group

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Chair

Niall Casey
Johnson & Johnson, USA

Stacey Halota
CISA, CISSP, CIPP, Graham Holdings, USA

Tammy Moskites
CISM, Venafi, USA

Lisa O'Connor
Accenture, USA

Ron Ritchey
JPMorgan Chase & Co., USA

Marcus Sachs
North American Electric Reliability Corporation, USA

Greg Witte
CISM, CISSP-ISSEP, PMP, G2 Inc., USA

Rogerio Winter
Brazilian Army, Brazil