ASA

Annie Searle & Associates LLC

Research Note

New Age of Cybersecurity: Rethink Cybersecurity Strategies and Implementation

Cory Shyu

October 2016

Keywords: Cybersecurity;

Abstract: The Internet of Things (IoT) has transformed the technology sector profoundly. While companies are rushing to reap benefits from increased productivity and automation by adopting more agile technology solutions, privacy and security issues have risen at an alarming rate. With recent high-profile data breaches across multiple industries, specifically the government, healthcare, retail, and financial services, companies have reprioritized security as a top objective. As a result, the security industry has experienced a surge in security budget allocation and interests in purchasing cybersecurity related products and services.

In the fast-paced IoT era, companies are experiencing new challenges associated with the increasing complexity in security management, including 1) exponential growth in number devices and heterogeneity of vendor sources, 2) obsolescence of security standard and guidelines, 3) higher vulnerability and increased response time, 4) increased sophistication of hacker techniques, and 5) trade-off between security and automation. To address these challenges, companies need a new approach to cybersecurity and change their mindset from reactive to proactive.

This paper addresses the key areas in which companies should rethink cybersecurity strategies and develop appropriate roadmaps to achieve security objectives. Companies should take the following actions to address the new industry challenges: reevaluate existing policies and procedures, analyze current gaps, strengthen security controls, enforce company-wide security trainings, and develop implantation plans for threat detection and response programs. Security controls must be implemented in line with business strategies and strike an appropriate balance with other constraints.

INTRODUCTION

Cyber-attack used to be a foreign concept and viewed as an extremely rare event. The network

sharing protocols were originally designed under the assumption of trust a few decades ago. Not long ago, cases of high profile data breaches have started to dominate headlines and people started to be conscious of the consequences of the lack of security in the internet era. Over a third of data breaches were caused by external hackers in 2013[1]. The magnitude of breaches has been astronomical, costing millions of dollars in legal damages and loss in revenues. According to a research note by Gartner[2], companies are more concerned about cybersecurity than ever before due to recent threats facing Target, Home Depot, and JP Morgan, etc. The large-scale data breaches were wake-up calls for top executives to reprioritize cybersecurity initiatives. Janice Newell, CIO of Providence Health & Services[3] mentioned that it is no longer a challenge to obtain budgets on strengthening security capabilities. Companies are contemplating the adoption of more resilient security systems. Gartner predicts that "by 2018, 40% of large enterprises will have formal plans to address aggressive cybersecurity business disruption attacks, up from 0% in 2015." (Procter, Witty, Litan, Perkins 2015)

KEY SECURITY OBJECTIVES

- Protect intellectual properties: Data theft is a source of major risk. Cyberattacks from China often target at security vulnerabilities to steal intellectual properties. Companies with large IP portfolios need to safeguard their intellectual properties against theft.
- Protect personal information: Employee and customer data are highly sensitive. According to Jenny Durkan Global Chair of the Cyber Law and Privacy Group at Quinn Emanuel Urquhart & Sullivan LLP, one hacker organization has allegedly stolen more than 100 million personal records. Identity theft is a growing concern in the healthcare industry.
- Protect financial information: Financial records often contain highly confidential competitive information. Companies face the risk of losing such information to competitors. The FBI's Cyber Division estimated that more than 500 million financial records have been stolen[4].
- Protect key operational data: Companies that process large volumes of transactions are sensitive to the risk of operational disruption. A halt in business operation can cost millions of dollars economic loss.

THE RISE OF ADVANCED PERSISTENT THREATS (APT)[5]

Security practitioners recognize the growing APT incidents which are more targeted and

[1] Biswas, "Data Center Security: Global Market," Nov 2015, BCC Research
[2] Procter, Witty, Litan, and Perkins, "Attack on Sony Pictures Is a Digital Game Changer," Feb 2015, Gartner
[3] "Business in the Age of Cyber Threats" conference, Dec 8, 2015, organized by the Foster School of Business
[4] "2015 Second Annual Data Breach Industry Forecast," 2015, Experian Data Breach Resolution
[5] Pingree, MacDonald, and Firstbrook, "Best Practices for Detecting and Mitigating Advanced Persistent Threats," May 4 2015, Gartner

malicious and often bypass traditional security controls. The scale and scope of security compromises from APTs are much more disruptive to business operations. The advent of APT requires companies to think beyond traditional security strategies and calls for security innovations.

NEW CHALLENGES IN THE CYBERSECURITY LANDSCAPE

Mind Commerce points out the major trends in IoT which have significantly impacted the challenges in cybersecurity[6].

- Exponential growth in number devices and heterogeneity of vendor sources: The increased complexity arisen from the proliferation of devices has a major impact on the access control protocols and security deployments because devices come from a variety of vendors with different hardware and security standards.
- Obsolescence of security standard and guidelines: Security and privacy standards are absent in the age of IoT. Most IoT devices were already in the market without proper security measures and new devices are introduced constantly. Policies and standards have not been in pace with the rapid changes in technologies.
- Higher vulnerability and increased response time: The increased adoption of big data infrastructure such as cloud has resulted in new challenges in data privacy and security. The data being handled often contain highly sensitive information such as intellectual property, password, and personal and financial information. The extent and scope of potential damages have grown exponentially. The consequences of data compromises are much damaging. This results in long lags between data breach and company response time. According to Center for Strategic & International Studies (CSIS), "85% of breaches took months to be discovered," and the average time is five months[7].
- Increased sophistication of hacker techniques: The digital age has introduced advanced techniques. Hackers have taken advantage of advanced tools to disrupt critical business operations. According to Kirk Bailey, CISO of University of Washington, there is a clear gap between company preparedness and hacker capabilities.
- Trade-off between security and automation: The utilization of cloud computing platforms can be a source of competitive advantage. However, the use of 3rd party platforms and software introduces new security risks. Companies often ignore the implications of critical liability clauses and access controls in service contracts. This issue is often cited by Fortune 500 IT leaders as a major source of risk.

REGULATIONS

[6] "Security and Privacy in the Internet of Things (IoT) Challenges, Market Opportunities and Forecast 2015 – 2020," (2015) Mind Commerce Publishing

[7] Lewis, James, "Raising the Bar for Cybersecurity," Feb 12, 2013, CSIS

As data breach became more prevalent, policymakers have raised standards and mandated disclosure requirements. Most notably, the SEC required proper disclosure on data breaches in 2011. The costs associated with increased scrutiny and auditing can be expensive for large public companies. While federal regulatory requirement on data breaches has still been in development, state-level regulations are likely to be in effect in the upcoming years. (Experian 2015) Joseph Lindstrom, GM of Information Security and Risk Management at Microsoft said that it's a matter of "when" cybersecurity becomes a regulation issue.

CURRENT STATE OF CYBERSECURITY PRACTICES

- Gap between perception and execution: According to a research surveying more than 500 C-level executives, 90%-95% stated that they saw values in investing in security infrastructures, but less than 50% of them stated that they were actively involved[8]. A CSIS survey showed that 45% of the surveyed companies believed they did well, however only 10% were taking adequate steps. (Lewis 2013)
- Absence of threat detection programs: According to GISS surveys conducted by Ernst & Young in 2014[9], 36% of respondents did not have a threat intelligence program; further 26% stated that their data protection policies were "ad-hoc" or "informal". In addition, 56% stated that it is unlikely their organization could detect sophisticated attack; 63% of organizations would take more than an hour to detect an attack. (Ernst & Young 2014)
- A surge in adoption of cybersecurity insurance: "According to the Ponemon Institute, the adoption rate for cyber insurance more than doubled from 10% to 26% over the past year[10]." A further study by Gartner showed that 33% of the companies plan to purchase cyberinsurance in the next 12 months[11]. While cyberinsurance can mitigate the magnitude of potential risks, it does not address the fundamental issues. Cyberinsurance should be used to address unavoidable risks in combination with building solid internal security infrastructure.

RETHINK SECURITY STRATEGIES AND IMPLEMENTATIONS

As mentioned previously, the rapid changes in the technology landscape have introduced new challenges to information security. The majority of companies have not been able to keep their policies and procedures up-to-date. To get started, companies should reexamine their security practices as follows:

- Assess and prioritize company information assets: The first question to address is, what

[8] "Business in the Age of Cyber Threats" conference, Dec 8, 2015, organized by the Foster School of Business
[9] "Cyber threat intelligence – how to get ahead of cybercrime", Nov 2014, Ernst & Young Insights on governance, risk and compliance
[10] "Aftermath of a Mega Data Breach: Consumer Sentiment," Ponemon Institute, May 2014
[11] Wheeler, Akshay, and Proctor, "Understanding When and How to Use Cyberinsurance Effectively," Mar 12 2015, Gartner

are the most sensitive data and where are they located[12]? And most importantly, what is the risk appetite for potential breaches? Survey shows that only 29% of companies have a complete inventory of data they own, and the percentage is declining due to the explosion of data volume. (Lewis 2013) A seemingly simple question can be a challenge to answer. Companies should consider the cost of losing data, regulation, and the nature of data and develop a priority list based on the assessments.

- Reassess existing policy and procedures for handling critical business data: New tools continue to be created and are often adopted too fast. Data security risks should be reassessed in pace with adoption of new technologies. Companies should rethink the trade-off between speed and security, then ask themselves which data should be automated and which shouldn't. There are thousands of technology solution vendors, each with different policies and standards on security. The consequences of mishandling data can be serious and should be reevaluated frequently.
- Reevaluate bring your own device (BYOD) policies: In the digital age, employees often bring their own devices to work. 57% of companies consider employees to be the most likely source of attack. (Ernst & Young 2014) This fosters the need for tightened endpoint control. Companies should develop clear guidelines on the use of personal devices.
- Strengthen security control procedures: Having an effective patch management process is the foremost important control according to Gartner. (Gartner 2015) "96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls." (Lewis 2013) The research findings are astonishing, indicating common weaknesses in existing security controls. Most companies fail even at the basic level. The fundamental controls such as patch, monitoring, and whitelisting applications should not be ignored.
- Implement routine company-wide security training programs: In the Business in the Age of Cyber Threats conference, senior security executives all emphasized the importance of changing attitude toward security – specially, security should be treated as an operational issue. Security hygiene should be routine and needs company-wide awareness. Appropriate data security policy training programs should be in place and update-to-date.
- Develop threat detection and response programs: Instead of being reactive to cyber-attacks, companies should explore advanced detection techniques and designate response teams to handle incidents timely. The team that handles incidents should develop proper response plans.

THE FIVE SECURITY OPERATIONS CENTER MODELS (SOC)[13]

[12] Loveland and Lobel, "Cybersecurity: The new priority," 2012, PWC
[13] Rochford, Lawson, "The Five Models of Security Operation Centers," Oct 22, 2015, Gartner

To implement a sound security practice, companies need to consider building proper SOCs. The primary objective of an SOC is to manage threat detection, response and prevention capabilities with centralized security operations functions and to ensure continuous monitoring of previously mentioned key security implementations. Gartner predicts that "by 2019, 50% of all security operations work in large and midsize enterprises will be conducted out of an owned or a shared security operations center, up from 15% in 2015." Gartner suggests 5 models of SOC to fit different organizational needs:

- Virtual SOC: A virtual SOC has no dedicated facility with only part-time team members and is reactive in nature. This model is the least mature among all SOC models and may be suitable for small businesses who expect infrequent incidents. This model can also be adopted as an interim approach for transitioning into more dedicated SOC model.
- Multifunctional SOC: A multifunctional SOC has dedicated facility and team members to perform security and other critical 24/7 IT operations. This model may be suitable for small, midsize and low-risk large enterprises when the respective functions are already performed by the same team members. While this model can does not require large capital outlay compared to some other dedicated models, the primary risks with this model is that politics, budget, process maturity levels can hinder execution.
- Distributed SOC: This model has dedicated and semi-dedicated team members which typically run during business hours. It is co-managed by managed security service providers (MSSP). This model may be suitable for small to midsize businesses. The primary driver for the adoption of this model are talent shortage, budget restrictions, and the considerable cost of 24/7 operations. Thus, having an in-house 5x8 operation with an MSSP covering non-business hours is a popular choice for larger organizations.
- Dedicated SOC: This model has a fully in-house dedicated facility and team which runs 24/7. A dedicated SOC is self-contained and possesses continuous day-to-day security operations. The team is typically composed of in-house security engineers, security analysts and a SOC manager. This model is typically used by large enterprises, service providers, and high risk organizations with multiple business units and geographically dispersed locations. This model is much more expensive than the other models due to higher personnel costs.
- Command SOC: This SOC model coordinates other SOCs and provides threat intelligence expertise. When an organization has multiple SOCs, there is a need to designate a command SOC which coordinates and manages other SOCs hierarchically. This model may be suitable for very large enterprises and service providers, governments, and military.

OTHER CONSIDERATIONS

- Cost-benefit assessment: No system is perfect and it is impossible to protect every asset. The use of advanced cybersecurity technologies can only mitigate, but not eliminate risks.

Also, there is a trade-off between increased security and individual privacy as well as the speed of getting work done. When tightening controls, the two get compromised and the right balance should be considered.

- Silo management: The silos between network control systems and endpoint are primary challenges for organizations to respond to advanced attacks effectively. When organizations move from a less centralized SOC toward a more centralized SOC model, there should be proper changes in process, policy, and organization structures.

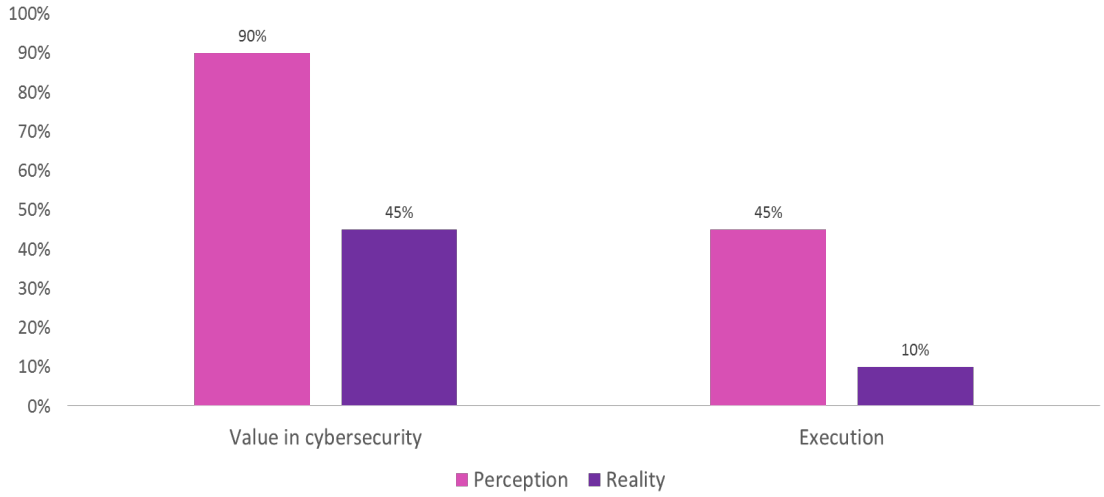
RECOMMENDATIONS

Satya Nadella said, cybersecurity is like going to the gym and must be exercised daily. Cybersecurity is no longer an IT issue, but requires company-wide awareness and appropriate implementation. Recent large-scale targeted attacks have prompted numerous conversations among top-executives regarding where they should start. I recommend a six-step action plan to rethink and address potential cybersecurity risks:

1. Develop priority list for key assets: Companies need to identify the key areas with the least risk tolerance and prioritize asset protection mechanisms in the event of attack.
2. Reevaluate policy and procedures: Employee BYOD and 3rd party vendor management are among the top security concerns among security executives. Vendor service agreement and liability sharing clauses are the primary source of dispute when data security is compromised. Companies need to reevaluate the potential vulnerabilities and current policies and procedures.
3. Analyze current gaps: After reassessment of current policies and procedures, the next step is gap analysis. Companies need to ask what needs to be done and how to bridge the gaps.
4. Strengthen security controls: Security hygiene can mitigate more 90% of potential data breaches. Companies should conduct routine re-examination and audit of existing security practices.
5. Enforce company-wide security trainings: Data breaches can come from a variety of sources. Given that hackers can easily search for vulnerabilities, breaches can happen anywhere in an organization. Therefore, companies must conduct up-to-date security trainings to all employees.
6. Develop implantation plans for threat detection and response programs: The implementation of SOC is critical to ensuring continuous monitoring of security controls. This is especially an important step to become proactive rather than reactive. Companies should consider the costs and benefits of the different SOC models and select the most appropriate one to meet their specific needs.

APPENDIX

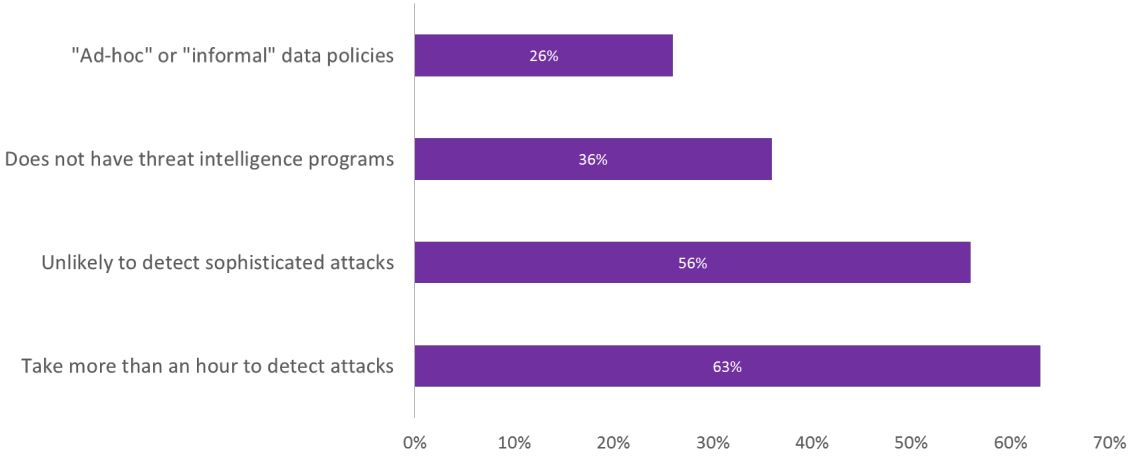
I. Gap between perception and reality



Source

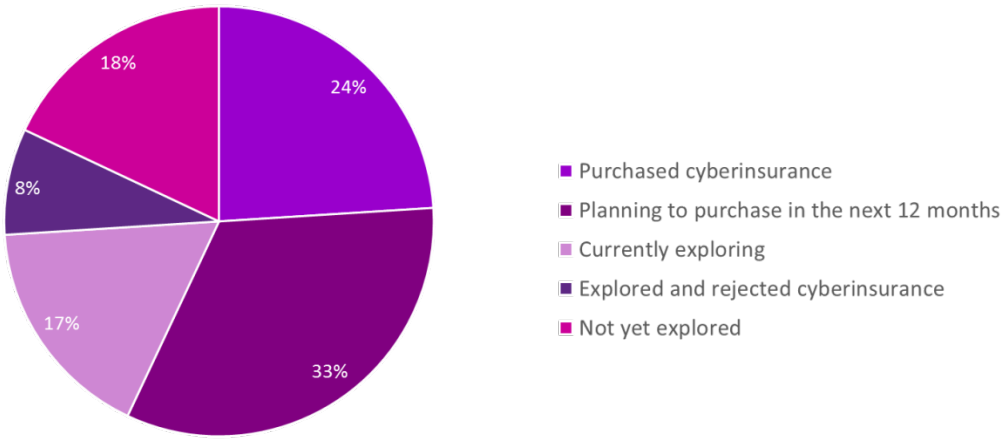
1. "Business in the Age of Cyber Threats" conference, Dec 8, 2015, organized by the Foster School of Business
2. Lewis, James, "Raising the Bar for Cybersecurity," Feb 12, 2013, CSIS

II. Absence of threat detection programs



Source: Sources: "Cyber threat intelligence – how to get ahead of cybercrime", Nov 2014, Ernst & Young Insights on governance, risk and compliance

III. Status of cyberinsurance adoption



Source: Wheeler, Akshay, and Proctor, "Understanding When and How to Use Cyberinsurance Effectively," Mar 12 2015, Gartner