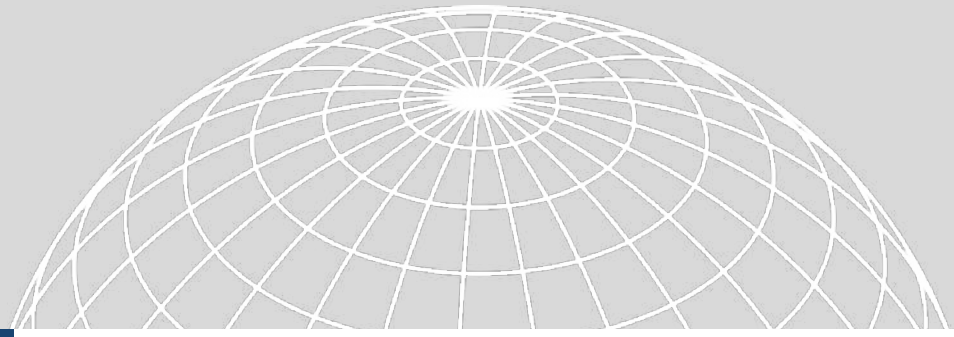


DEVELOPING A CYBERSECURITY MINDSET IN THE C-SUITE

MARK INBODEN,
PRESIDENT & CEO

UCEC SMART™

Executive Summary

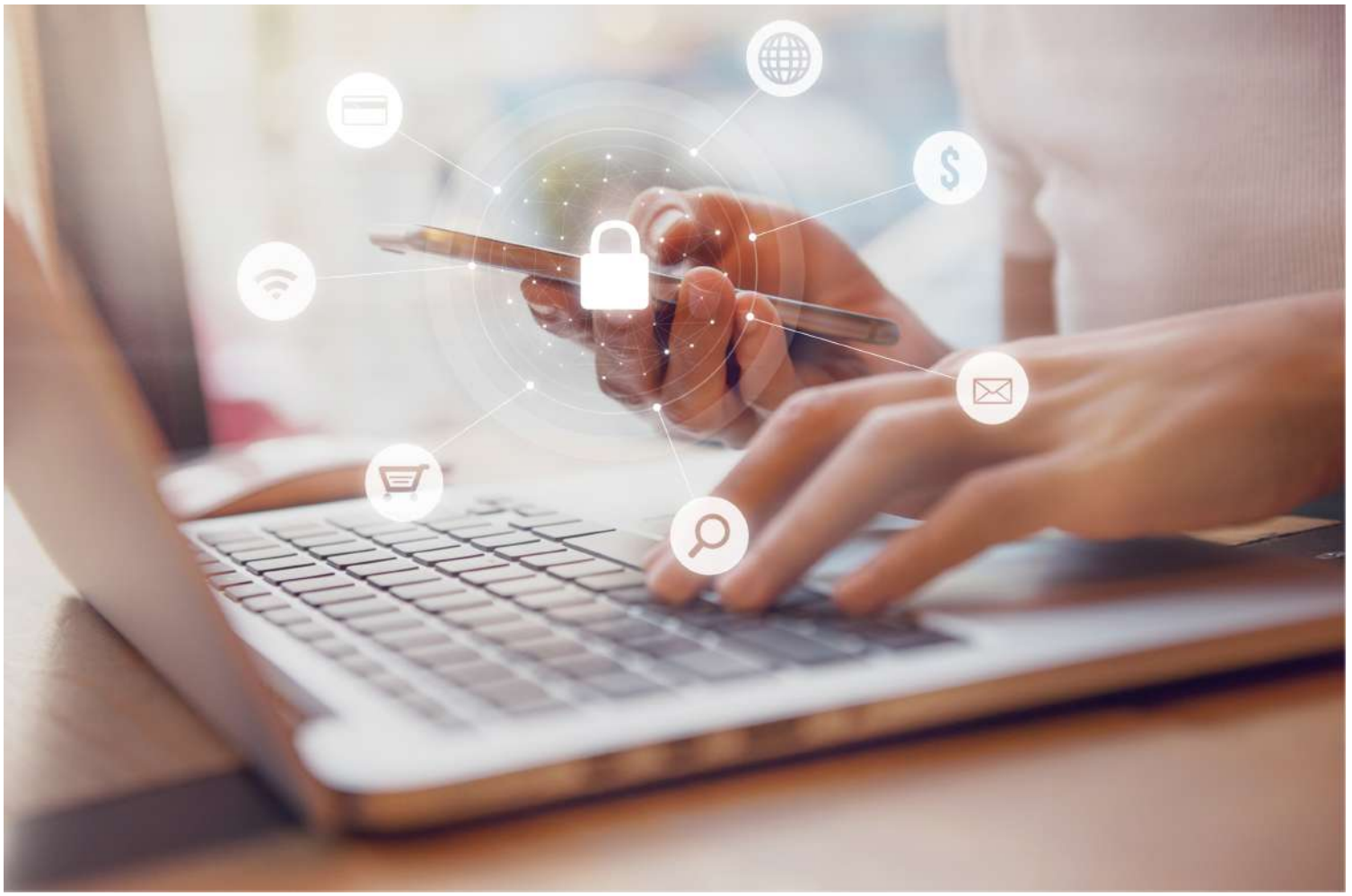
As the President and CEO of a manufacturing company involved with the Internet of Things (IoT) space, I know that IoT is not only a great growth industry, but also presents even greater cyber security risks that are not being addressed by traditional IT thinking. This guide is purposely a "non-technical" paper directed at "C-Suite" occupants. Few in the "C-Suite" have a computer science or engineering background, but the data to run their businesses and make business decisions is being shaped by the daily deployment of IOT technologies. With that said, it is imperative for "C-Suite" occupants to have a basic understanding of not only the technologies utilized in their organizations, but also the potential threats and risks. Managing the complexity of disparate systems and associated security is more difficult than ever, and should not rest entirely on the shoulders of the CIO, or his/her IT deputies. The "C-suite" is ultimately accountable to a company's board, shareholders, and customers. Developing a security mindset is paramount to success.

The C-Suite & Cyber Security

Building and Developing a Cyber Security Mindset among C-Suite level executives is critical to future business success. The C-Suite is ultimately accountable to a company's board, shareholders and customers.

C-level titles are used to describe a highly ranked individual's role within the company. Corporate titles are used to indicate his or her responsibility within a company. Officers and managers that maintain C-level positions are some of the most influential and dominant members of an organization.[1] These positions have traditionally been focused on company profitability, growth, and shareholder returns. With increasing reliance on emerging technologies to deliver even better bottom-line results, the positive and negative risks associated with these technologies needs to be well understood. According to a recent study conducted by NC State's Poole College of Management, however 80% of organizations surveyed from all over the world have no formal risk training for executives.[2] Most executives are willing to "place a bet" on a technology that improves profitability. The ROI on any technology initiative must also be evaluated in terms of the cyber risk involved. The C-suite must educate itself on these potential risks and lead in the development a formalized plan to ensure risk evaluation is a mandatory component of existing and proposed technologies.

> *80% of organizations have no formal risk training for executives.*



IoT Risk

"In 2015, Juniper Research predicted that the continued reliance on digitization in our lives will be the catalyst for a $2.1 trillion criminally driven industry by 2019."[4] Where does the C-Suite start to address the potential risk for their organization?

Risk assessment, minimization, and monitoring must become a concrete agenda item in every C-Suite meeting. A recent PwC report, "The Global State of Information Security Survey 2018, which surveyed more than 9,500 executives in 122 countries, found that 44% don't have an overall information security strategy and 48% don't have an employee security awareness training program."[3] Traditionally, IT departments were tasked with securing networks and communications. The Internet of Things (IoT) has placed demands on businesses to open up historically proprietary systems to new externally based technology, often without a prior assessment of new risks that will emerge with the advanced in technology. As organizations rely more on real-time data analytics, it becomes paramount that the entire organization adopts a security first mindset, as discussed in our class.

A company must be very clear in what it is working to protect. Platforms, Software, and Services are a good place to start. Employees interact with all of these during the course of their day. Device management, Application management, and Network management platforms all show a greater than 25% CAGR according to the class slide below:

SPOTLIGHT

FIGURE 33 DEVICE MANAGEMENT PLATFORM EXPECTED TO LEAD THE IOT TECHNOLOGY MARKET DURING THE FORECAST PERIOD

	Device Management Platform	Application Management Platform	Network Management Platform
2016-e	2.96	2.05	1.46
2022-p	15.34	8.84	5.65
CAGR (2016-2022)	31.5%	27.5%	25.2%

5 *CAGR=Compound Annual Growth Rate

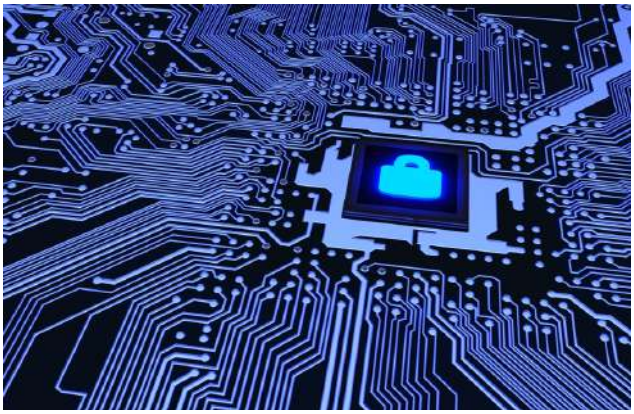
C-Suite members must also understand which digital assets are at risk. "As businesses have become more automated and data driven, they are creating more valuable digital assets. These are groupings of data that, if compromised, could have serious negative financial, reputational, legal or compliance implications."[6] Because assets are located in all operational areas each C-Suite member must develop a formalized process to fully understand risks in their area of responsibility. By regularly tasking internal stakeholders in these areas with risk assessment identification, the C-Suite can become a collaborative force in identifying risks at all levels of the organization.

The Threat Mindset

"Traditional security doesn't meet all of IoT's security needs," says Chris Penrose, senior vice president for Internet of Things Solutions at AT&T. "Unfortunately not all users think about new security risks and simply follow the Security practices that they have always used." [8]

The focal point of this course is in developing a security mindset. As IoT devices become more prevalent in our businesses, this mindset needs to be at the forefront of an integrity review of every data interaction, inclusive of completely internal interactions and those involving an external entity.

We were encouraged to use Orthogonal thinking, "Which draws from a variety of, and perhaps seemingly unrelated, perspectives to achieve new insights. It is the even momentary blurring of boundaries to see what might emerge"[7] Utilizing this concept, we should apply it to cybersecurity, by looking to understand the threat mindset that is at the core of cyber criminals.

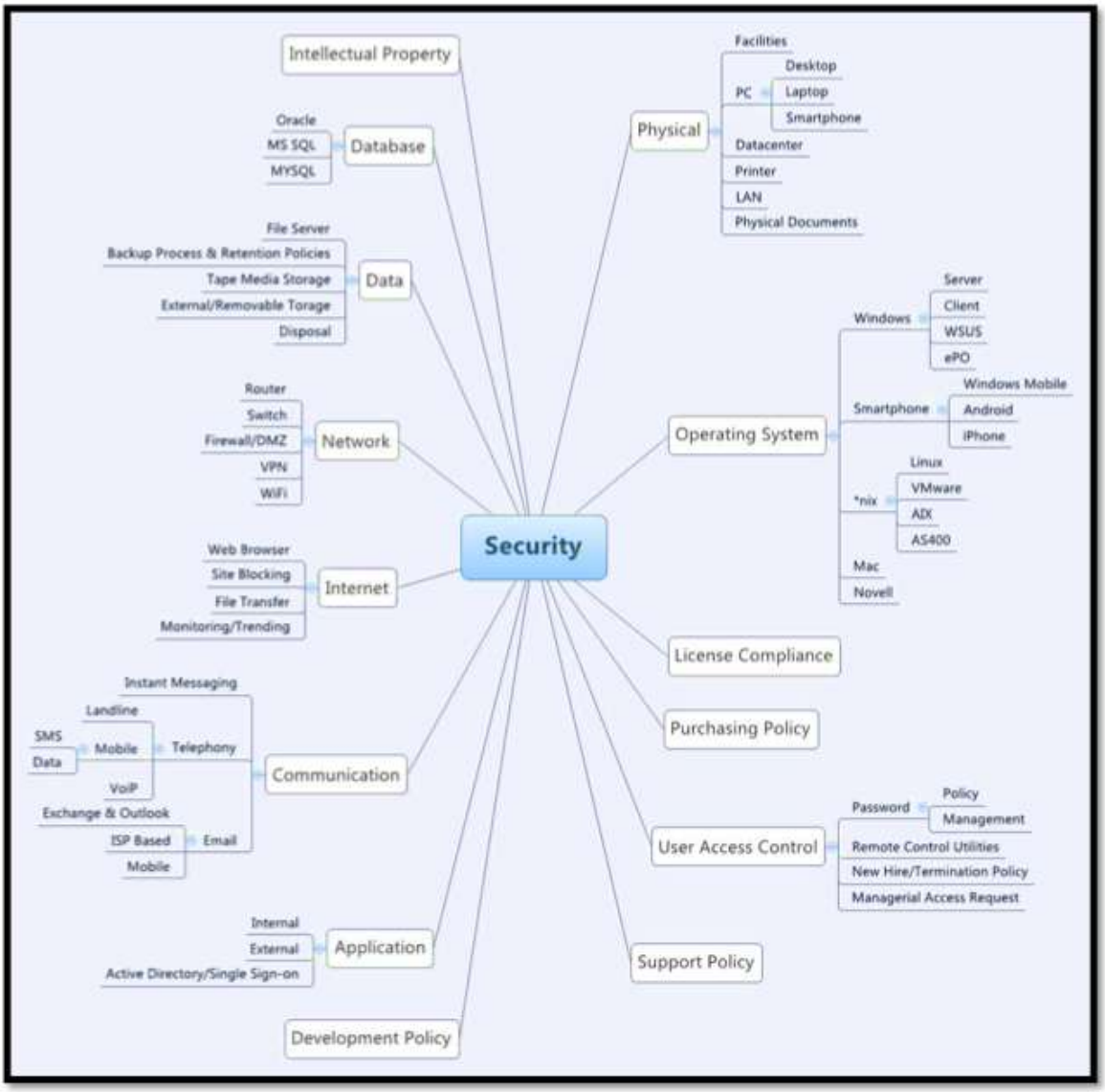


Cyber criminals are constantly creating looking at new methods to attack and penetrate security systems. Historically, most C-Suites have relied on implementing the latest and greatest security prevention technology available.

It is quite unnerving that cyber criminals have a diligent day-in and day-out work ethic focused on breaching the corporate security walls.

Cyber criminals are adept at looking at this orthogonally, knowing that one successful penetration often leads to a path of a mother lode of readily marketable data. These criminals quickly sift through the data and immediately look to the dark web to monetize. C-Suite executives place a high value on company performance metrics. Cyber criminals, in contrast, are interested in supplier, client, and employee information that has a liquid, lucrative black market.

The mind map below is representative of security traditionally deployed in organizations. By looking at this map from the oppositional viewpoint of a cyber criminal assessing opportunities, an organization can better determine where security issues may exist.



Mobile First Paradigm

By the end of this decade, over one-third of all data will reside in or pass through the cloud.[10] IoT is expanding into all areas of our lives. Worldwide by 2021, there will be 25.1 billion internet-connected devices, growing at a rate of 32% per year. [11]

Having access to your business, via the cloud, from your phone is convenient, but it poses risks. Man-in-the-middle attacks, whereby a third party secretly intercepts a message and sometimes modifies the message content for malicious reasons are a major concern. Public Wi-Fi hot spots by employees are vulnerable to Man-in-the-middle attacks. Malware is being targeted at mobile devices by being surreptitiously imbedded in offerings in app stores. Company emails and applications can be unknowingly exposed while waiting for a flight or a meeting at a coffee shop. Encryption, MACs, and Hashing should be utilized at the highest appropriate level based on the value of the data being transmitted and the transmission technology involved.

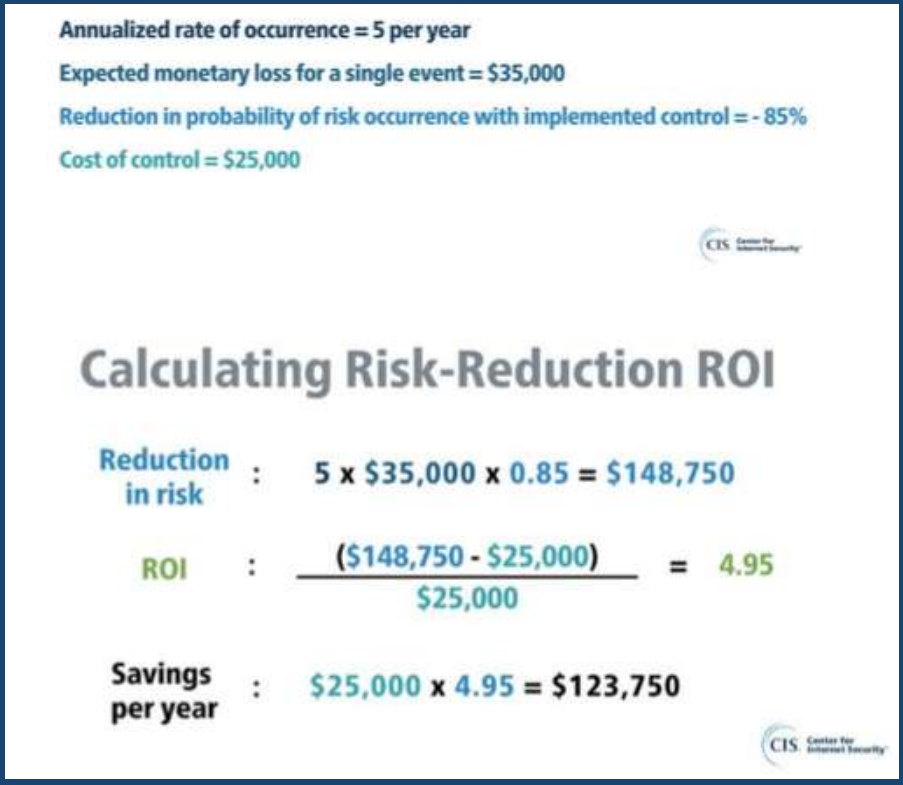
A staggering 91 percent of cybercrime starts with email, according to a 2018 report by security firm FireEye.[12] Email is the lifeblood of any organization, but is often one of the least prioritized applications from a security standpoint. Phishing, Malware, Spyware, and Impersonation are among many of the attacks being perpetrated in the email arena. In fact, email users are three times more likely to respond to a phishing attack on a mobile device than a desktop, according to an IBM study — in part simply because a mobile device is where people are most likely to first see a message.[13] With multiple accounts on personal devices, work and personal emails can often look alike. It's automatic to open an email with a familiar looking name, and only later find out that it was "spoofed" and a virus is now a companywide problem. Again, the C-Suite must address these potential problems with complimentary policies and technology.

Reducing Risk

Education and training on cyber security must start with a commitment from the top of the organization. The C-Suite needs to ensure that all levels of the company are appropriately trained and informed on the threat of cyber-attacks. Once training, risk assessment and policies are in place, continual monitoring and commitment to cyber protection is required. The cost of implementing a cyber security protocol has typically not been a "line item" in the corporate budget. The following example illustrates the ROI on cybersecurity training:

A Closer Look at ROI: Phishing Attacks

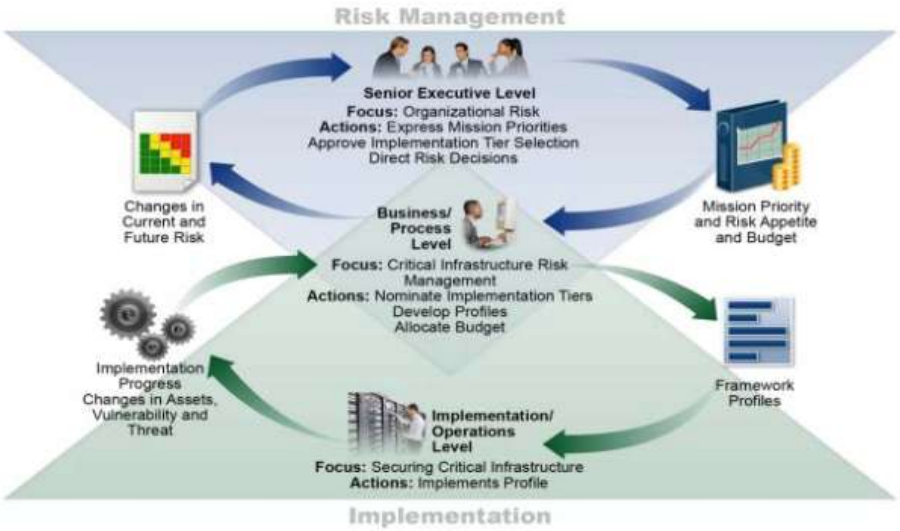
Your organization can expect to get phished 5 times per year, at an estimated cost of $35,000 per successful attack. The cost to train employees to spot and avoid phishing emails is expected to be $25,000. Here's what the security ROI would look like [14]:



This ROI equation is powerful enough for any C-Suite member to get onboard in promoting training to reduce cyber threats and potential loss to their business.

Establishing a Program

Where to start? NIST, the National Institute of Standards and Technology that is part of the U.S. Department of Commerce provides resources for cyber security including best practices, guidelines, and standards designed to protect the U.S. economy. The NIST "Framework for Improving Critical Infrastructure Cybersecurity v1.1"[15] provides a wealth of information that can be easily absorbed and delegated within the C-Suite. These two images capture an overall look at the process.



Conclusion

The best defense against the growing and ever-evolving cybersecurity threat is instilling a security mindset, first in the C-Suite and then companywide.

There is no perfect security system. The best defense is to develop and instill a security mindset, first in the C-Suite and then companywide. The financial justification for a comprehensive approach is compelling. Organizations engage outside resources for specific expertise in many operational areas and cyber security initiatives should be no different.

By starting at the C-Suite and then engaging all operational areas, employees at all levels, and outside cybersecurity experts, a company can effectively and efficiently chart a course to assess and address risks and threats. A comprehensive plan such as the NIST model to Identify, Protect, Detect, Respond, and Recover16 is vital to the digital health of any company.

C-Suite members do not have to become cybersecurity experts. Responsibility, however, does reside in the C-Suite and keeping this top of mind is vital to the success of the business, employees, customers and all stakeholders.

Endnotes

[1] What are C-Level Corporate Jobs https://www.thebalancecareers.com/what-are-c- level-jobs-2061934

[2] Preparing C-Level Employees to Address Risk https://www.riskmanagementmonitor.com/preparing-c-level-employees-for-risk/

[3] Strengthening digital society against cyber shocks
https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society- against-cyber-shocks.pdf

[4] CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019
https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses- over-2trillion

[5] Figure 33 Device Management Platform Expected to Lead the IoT Technology Market During the Forecast Period Industrial IoT Markets and Security University of Colorado Boulder Professor David Sluiter

[6] Cybersecurity: What manufacturing CEOs Need to Know https://www.aprio.com/cybersecurity-ceos-need-know/

[7]Orthogonal Thinking & Doing
http://interactioninstitute.org/orthogonal-thinking-and-doing/

[8] The CEO's Guide to Navigating the Threat Landscape
https://www.business.att.com/content/dam/attbusiness/reports/vol4-threatlandscape.pdf

[9] Security Mind Map Illustration https://www.4kepics.com/mind-map-security

[10] CSC Insights – Big Data Just Beginning to Explode
https://visual.ly/community/infographic/technology/big-data-just-beginning-explode

[11] How to Secure the Enterprise Against the Internet of Things Onslaught
https://www.gartner.com/doc/3895598?ref=mrktg-srch

[12]Email Threat Report https://www.fireeye.com/offers/rpt-email-threat-report.html 13Mobile Users 3 Times More Vulnerable to Phishing Attacks https://securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing- attacks/

[14]A CISO's Guide to Bolstering Cybersecurity Posture
https://www.cisecurity.org/resources/white-papers

[15] Framework for Improving Critical Infrastructure Cybersecurity
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[16]Framework for Improving Critical Infrastructure Cybersecurity
https://www.nist.gov/cyberframework/framework-resources-0