2015

S2R Execution Bridge LLC
strategy|technology|consulting

Linda Hutchinson, CISM® Candidate

Keeping Information Security Simple for SMBs™

SMB DATA SECURITY CYBER COMMANDMENTS

Cyber risk is a given in today's hyper connected business world. All companies that are connected to the Internet have an underlying and unavoidable cyber risk factor. Start the journey toward a more secure business with the SMB Data Security Cyber Commandments.

SMB Data Security Cyber Commandments

Executive Summary

Cyber risk is a given in today's hyper connected business world. All companies that are connected to the Internet and using digital resources (computers, networks, mobile devices, electronic sensors, software, etc.) of any kind have an underlying and unavoidable cyber risk factor. But how can small and medium business (SMB) owners keep hackers out of their data when large enterprises like Anthem[1], Sony[2], and Target[3] can't seem to keep their systems secure?

The majority of SMB owners recognize that they need to do more to protect their data, but they often struggle with ***what*** to do, ***how*** to do it cost effectively, and ***who*** is going to do the work for them. A critical first step is recognizing that effective security is about governing **people, process, technology**, and **risk management** appropriately. Mastering the people and risk management aspect of data security via strong governance means that adopting even basic technical controls and process improvements will yield meaningful results.

SMBs should begin by adopting the risk management practices and implementing the baseline technical safeguards recommended in the SMB Data Security Cyber Commandments™.

SMB Data Security Cyber Commandments™ (CCMD)

1. **Thou Shalt Know Thy Assets, Risk Environment, and Risk Appetite**
2. **Honor Thy Data**
3. **Thou Shalt Know Thy Threat Landscape**
4. **Remember Thy People & Honor Them with Education**
5. **Thou Shalt Know Thy Network**
6. **Honor Thy Code**
7. **Remember to Keep Thy Network, Devices, Apps, & OS's Patched, Updated, and Holy**
8. **Thou Shalt Trust Only What is Known to be True**
9. **Thou Shalt Adopt a Least Privilege Approach to Data Access and User Rights**
10. **Remember Thy Connected Systems, Processes, and Business Interactions**
11. **Thou Shalt Balance Prevention, Detection, Response, & Recovery Investments**
12. **Keep Sacred the CIS Critical Security Controls[4]**

[1] "Statement Regarding Cyber Attack Against Anthem." *Anthem Blue Cross Blue Shield.* (Feb. 2015) WEB. July 2015. <www.anthem.com>
[2] Sanders, James. "Sony Pictures Hack: Employee Information and Unreleased Films Leaked." *Tech Republic*. (Dec. 2014) WEB. July 2015. <www.techrepublic.com>
[3] Kassner, Michael. "Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned." *ZDNet Special Feature*. (Feb. 2015) WEB. July 2015. <www.zdnet.com>
[4] *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*. Center for Internet Security. Oct. 2015 Retrieved from <www.cisecurity.org>

SMB Data Security Cyber Commandments

The SMB Data Security Cyber Commandments™ are meant to help SMBs think about what needs to be addressed to properly prepare for cyber attacks and likely breaches. Instead of requiring guru level technical expertise, they require being an expert on your business environment, having a deep understanding of your business data flows, and an accurate view of its network connections, authorized devices, and "in use" applications. Success depends on: knowing and controlling what information is being collected, used, and stored; understanding how the business' data flows across systems, within applications and processes, between connected networks, and to the intended people across all of their authorized devices; and on the data security engagement level and risk management attitude of the entire organization. Success also depends on recognizing that you cannot outsource the business ownership and responsibility of data security to either the internal IT team or to an external third party. You can only outsource some of the tactical implementation and operational services associated with it.

Business owners and key stakeholders should discuss the SMB Data Security Cyber Commandments™ with their existing team of trusted advisors - technology service providers, lawyers, accountants, merchant bankers, and financial services advisors. They should leverage those professional relationships to help them access the cyber risks for their business and to start the process of implementing a data security program. SMBs should augment their advisors with data security professionals where needed to ensure a comprehensive risk assessment is shaping their information security program and associated controls. It's important to remember that data security is a marathon that requires commitment and constant attention. Tackle it in measured phases taking into account the highest risk factors, company culture and capabilities, and existing controls while moving to a more security conscious organization over the long haul.

The SMB Data Security Cyber Commandments™ reflect the intertwined nature of risk management, people, process and technology components that together build a secure and effective business system. Embracing them can guide your company toward reaching the optimal information security maturity stage appropriate for your business risk environment.

The SMB Security Dilemma

Each new day seems to bring a new data breach headline. OPM[5], Anthem[6], and Ashley Madison[7] have all been recently added to the latest cyber roadkill list. It's enough to make small and medium business (SMB) owners turn pale when thinking that if big organizations like these can't stay secured in spite of all of their security investments, how is a little guy supposed to keep hackers' prying eyes and stealing tentacles out of their data treasure troves?

The answer is often easier said than done. The majority of SMB owners recognize that they need to do more to protect their data but they struggle with ***what*** to do, ***how*** to do it cost effectively, and ***who*** is going to do the work for them. Small businesses have a natural tendency to look at data security as just another black hole that is a necessary evil driven by compliance needs instead of treating data security as a business enabler and top corporate priority. Reality is that their main concern is keeping the lights on. They just want to make enough money to handle their expenses, and have free cash flow leftover to reinvest in the business. They don't usually have a full time IT resource on staff. For the ones that do, the odds are those resources are good IT generalists and not necessarily information security specialists. To make matters worse, those they have tried a DIY data security approach can be stymied by the sheer volume of security standards, frameworks, and technical solutions available. It may leave them feeling overwhelmed when trying to understand it well enough to develop an actionable, affordable data security plan. Faced with complexity, costs, and limited resources, it should come as no surprise that many choose to ignore it completely or simply do the absolute minimum. They have entered into what the Center for Internet Security (CIS) calls the dreaded "Fog of More."[8]

There is no doubt that complexity and complacency are the enemies of data security. As an industry, we need to do a better job of helping SMBs navigate cyber space more confidently. It starts with taking the fear of not being a technical cyber expert out of the SMB security equation. Effective security starts with adequate governing of **people, process, technology**, and **risk management** through a business model for information security.[9] Technology is simply one aspect that not only creates a material part of the vulnerabilities but also brings innovative security controls into the mix. I believe that **people** are the biggest factor impacting data security, and that adequate risk management is a close second. Mastering the people and risk management aspect of data security via strong governance means that adopting even basic technical controls and process improvements will yield meaningful results.

---

[5] Davidson, Joe. "New OPM Data Breach Numbers Leave Federal Employees Anguished, Outraged." *Federal Eye - The Washington Post.* (July 2015) WEB. July 2015. <www.washingtonpost.com>

[6] "Statement Regarding Cyber Attack Against Anthem." *Anthem Blue Cross Blue Shield.* (Feb. 2015) WEB. July 2015. <www.anthem.com>

[7] Zetter.Kim. "Hackers Finally Post Stolen Ashley Madison Data." *Wired.* (Aug. 2015) WEB. Aug. 2015. <www.wired.com>

[8] *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*. Center for Internet Security. Oct. 2015 Retrieved from <www.cisecurity.org>

[9] *CISM Review Manual 2014.* ISACA. Pg. 37. 2014.

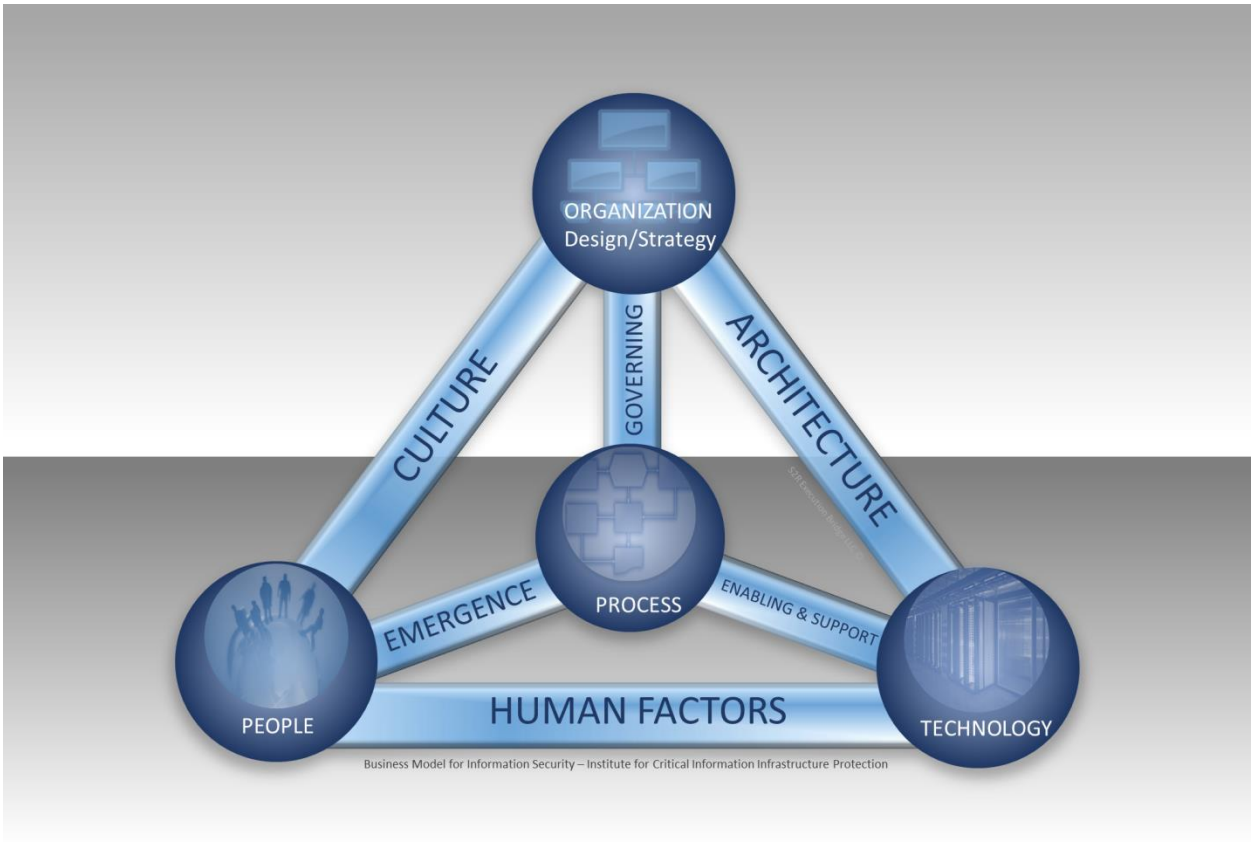

Figure 1: Business Model for Information Security - CISM Review Manual 2014, ISACA.

The challenge is not only in how to guide the SMB masses to the security risk management watering hole, but how to also encourage them to drink enough of the water of their own free will. The best place to start is helping them recognize the importance of cyber security to their main business objectives: generating and growing revenues, reducing costs, building a brand, maintaining a good reputation, and remaining an ongoing concern. Every business has these concerns but they are table stakes to SMBs because their ability to weather a cyber storm is different than a F500 company. A recent infographic from Champlain College estimates that more than half of U.S. business with revenues less than $10 million reported some type of data breach in 2013 with 60% of them failing within six months of a cyber attack.[10] That statistic alone should help reprioritize data security efforts within an SMB.

[10] Winfrey, Graham "Can your Company Survive a Cyber Attack? *Champlain College Graduate Studies Infographic.* Retrieved from Inc. (Dec. 2014.) WEB. Aug. 2015 <www.inc.com>

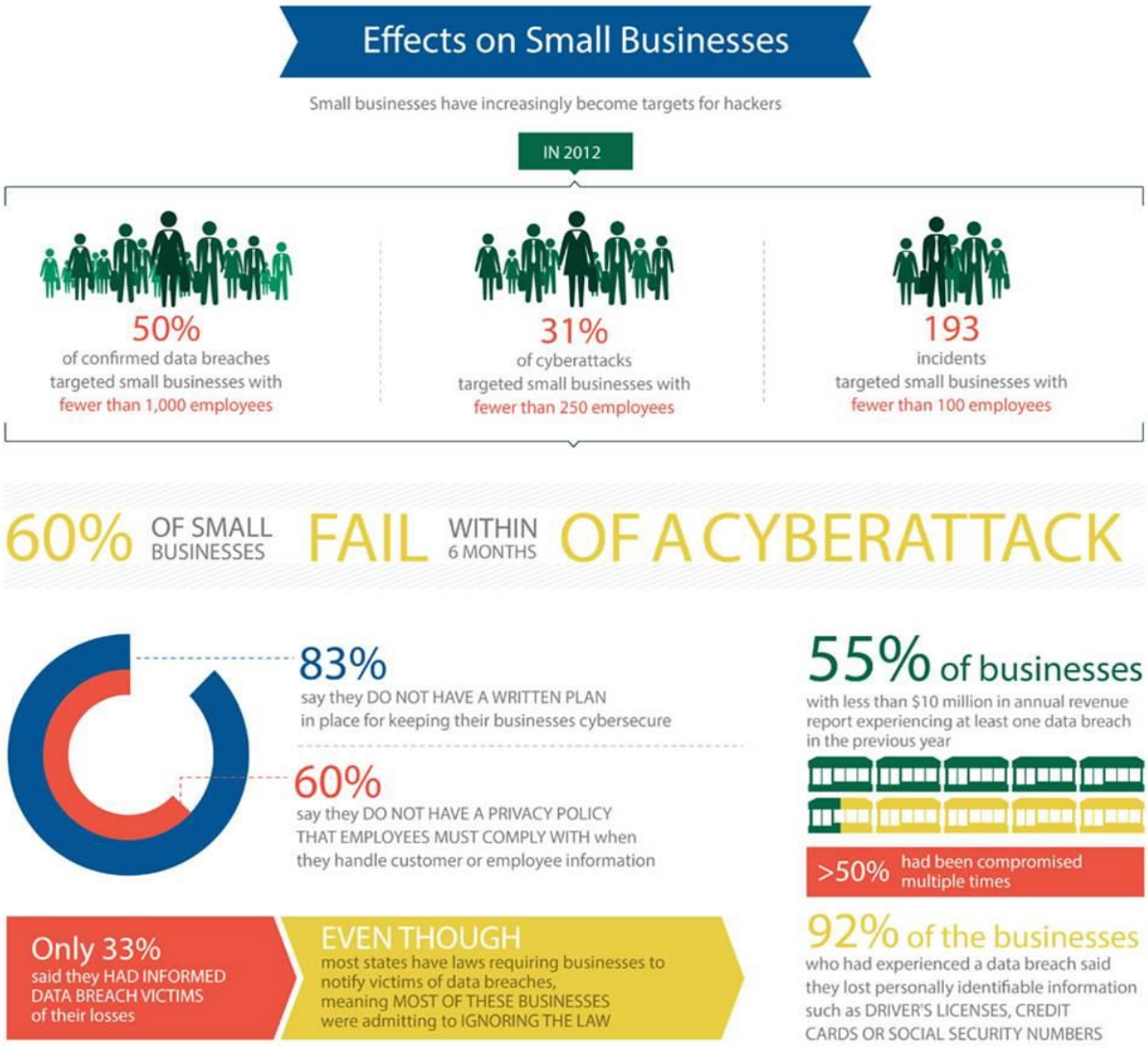

Figure 2: Champlain College Graduate Studies Infographic published December 5, 2014. Accessed 8/1/15 from www.inc.com.

Another important data point for SMB owners to know is what the cost of a data breach means to organizations of all sizes. The 2015 Verizon Data Breach Investigations Report included a breakdown of costs associated with data breaches based on the total number of records compromised. [11] Their analysis shows that it is more accurate to look at the cost of breach in this fashion than in using overall averages because the large breaches skewed the results too much on a per record basis. The Verizon research shows that even a small breach of 100 records can cost a business an average of $25,450 to handle. How many small businesses have an extra $25,000 around to cover responding to a breach?

[11] 2015 Data Breach Investigations Report – Executive Summary. *Verizon*. Retrieved from www.verizonenterprise.com. July 2015.

FIGURE 3 COST OF A BREACH BREAKDOWN

Records	Prediction (lower)	Average (lower)	Expected	Average (upper)	Prediction (upper)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Figure 3: 2015 Data Breach Investigations Report – Executive Summary. *Verizon*.

These two data points coupled with the breach liability shift in October 2015 associated with EMV credit card terminal adoption, should really give SMB owners pause to better understand the impact that poor data security management practices can have on their long term business viability. They clearly need to assess the appropriate level of data security investments they should be making, but where should they start?

SMBs should first adopt the risk management practices and implement the baseline technical safeguards recommended in the SMB Data Security Cyber Commandments™. Doing so will at least put their finger in the dike to stem the flood of attacks coming their way.

Three key tenets come to mind for adopting basic risk management practices and implementing baseline technical safeguards: 1] KNOW THYSELF, 2] KNOW THY ENEMIES, and 3] KNOW THY FRIENDS. Together they form the basis of the SMB Data Security Cyber Commandments™.

SMB Data Security Cyber Commandments™ (CCMD)

1. **Thou Shalt Know Thy Assets, Risk Environment, and Risk Appetite (THYSELF)**
2. **Honor Thy Data (THYSELF)**
3. **Thou Shalt Know Thy Threat Landscape (THY ENEMIES)**
4. **Remember Thy People & Honor Them with Education (THYSELF)**
5. **Thou Shalt Know Thy Network (THYSELF)**
6. **Honor Thy Code (THYSELF)**
7. **Remember to Keep Thy Network, Devices, Apps, & OS's Patched, Updated, and Holy (THYSELF)**
8. **Thou Shalt Trust Only What is Known to be True (THYSELF)**

9. **Thou Shalt Adopt a Least Privilege Approach to Data Access and User Rights (THYSELF)**
10. **Remember Thy Connected Systems, Processes, and Business Interactions (THYSELF & FRIENDS)**
11. **Thou Shalt Balance Prevention, Detection, Response, & Recovery Investments (THYSELF)**
12. **Keep Sacred the CIS Critical Security Controls [12] (THYSELF)**

While certainly a bit tongue in cheek and not terribly original, these SMB Data Security Cyber Commandments™ are meant to help SMBs think about what needs to be addressed in order to properly prepare for cyber attacks and likely breaches. Of note should be that most are risk management and governance related and don't involve being an IT expert or information security guru. They do, however, all involve being an expert on your business environment, having a deep understanding of your business data flows, and an accurate view of its network connections, authorized devices, and "in-use" applications. Success depends on: knowing and controlling what information is being collected, used, and stored; understanding how the business' data flows across systems, within applications and processes, between connected networks, and to the intended people across all of their authorized devices; and on the data security engagement level and risk management attitude of the entire organization.

A description of what each commandment addresses follows.

1. **CCMD-1: Thou Shalt Know Thy Assets, Risk Environment, and Risk Appetite**

   Everything starts with understanding the risks associated with a business, and its comfort level plus capability in addressing those risks. For any business, the risk environment consists of both internal and external factors. The external business environment involves the overall industry and market trends, competitive landscape, extended business ecosystem, financial markets, political arena, legal and regulatory bodies, customers, social and cultural norms, and investors. Besides firms having a general cyber risk exposure, there may also be a vertical specific added risk for critical infrastructure entities, and an additional high-value-target risk associated with a company's visibility, symbolism, and/or strategic relevance to a country, cause, or industry.

   The internal risk environment spans: key stakeholders including employees, executives, board members, connected ecosystem partners , integrated suppliers or service providers; company hierarchy; organizational culture; business drivers and strategy; human and capital resources; assets (property, data, systems, applications, processes, equipment, IPR, etc.); business plans, and the firm's capabilities and maturity. All businesses have a general insider cyber risk exposure with insiders being defined as not just employees but also third parties with access to the company's networks, data, and resources plus ecosystem partners like key suppliers and channels to market.

[12] *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*. Center for Internet Security. Oct. 2015 Retrieved from <www.cisecurity.org>

Combined the internal and external risk environment creates the Rings of Cyber Relationship Risk™. Generally the closer something is to the innermost ring, the higher level of cyber risk there will be to the organization.

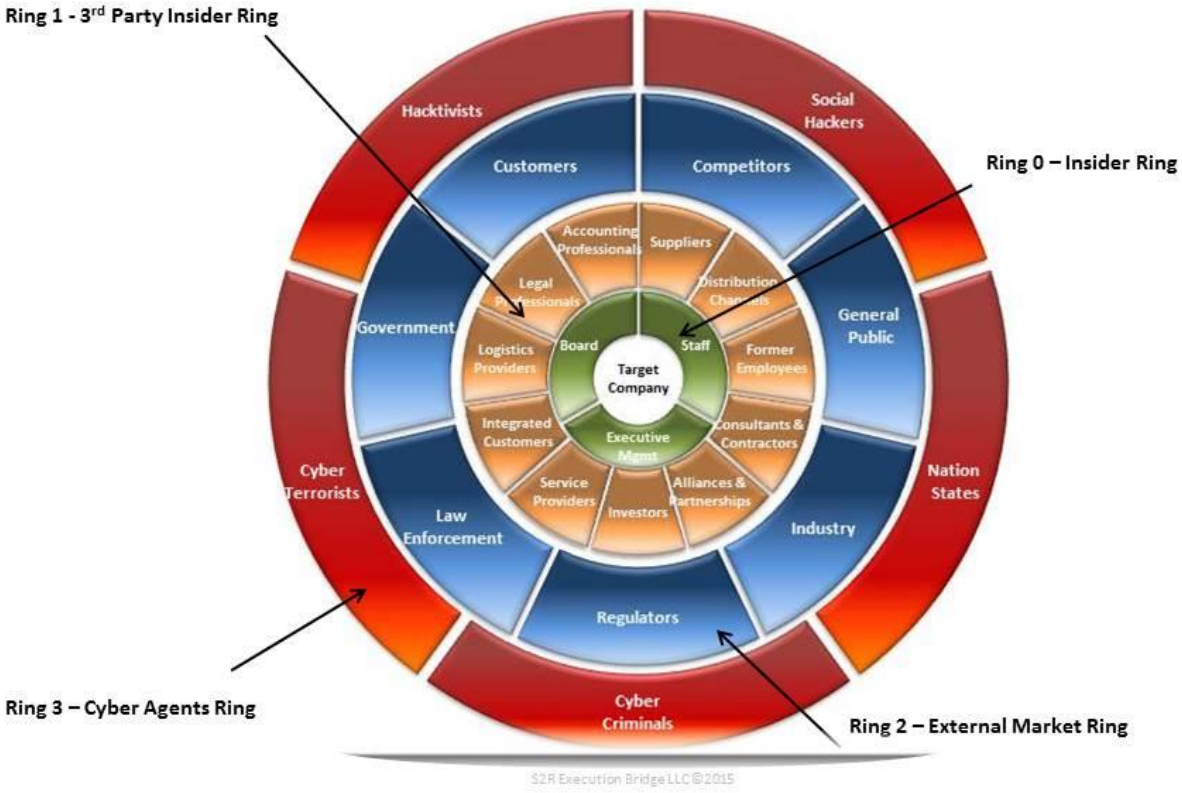

Figure 4: Rings of Cyber Relationship Risk

Risk appetite is simply the amount of risk that a firm is willing to accept in the course of conducting its business.[13] Conservative businesses have a low risk appetite while start-ups are generally more comfortable with a higher level of risk as the norm. Risk appetite drives an organization's risk culture which influences its overall culture, data security attitude, and business practices.

Recommended Actions

Start simple and identify the most critical assets to your business without which business operations cease to operate effectively. Brainstorm with other stakeholders and jointly select the top one to three business risks to those critical assets that have the highest likelihood of occurrence and

[13] See footnote 9

biggest impact to the business. Think about how general cyber risks could possibly trigger them. Think about how the top customers that drive your business would react to a breach of their networks due to a breach at your company. Think about potential legal and regulatory fallout from a breach. Consider how your business would continue to operate if you were a targeted victim like Sony[14] or Ashley Madison.[15] Take the time to research and fully understand the data security regulations and guidelines for your industry. How compliant do you need to be and are **willing** to be given the risks and the costs associated with stated requirements and your risk appetite? Auditors and regulators will cringe at the emphasis on the term "willing" but the degree of compliance to any law, regulation, or industry framework is fundamentally a business risk management decision.

Recognize that compliance does not equal security. You can be compliant with having a control in place that fulfills a specification in a standard but if the control is not being implemented effectively, you are not secure. True security goes beyond checking the compliance box. It must become a part of the company mindset and a strategic objective to be meaningful and material.

Consult with an attorney or other trusted advisor who is knowledgeable of your industry requirements and your business. Engage in a cyber risk assessment discussion with them. If your attorney or other trusted advisor is not yet cyber risk aware, augment their legal risk expertise with an information security risk management consultant that is willing to work in close concert with them to help you conduct a business risk assessment of your environment and help you craft an overall security policy that is right sized for your business. Think about worst case. Plan and prepare for the expected case based on your risk appetite. Hope for the best case while hedging your bets against worse case where it makes business sense to do so. Be sure to incorporate the cyber risk discussion into the firm's overall risk management processes. If you don't have an overall firm risk management process, make the effort to start implementing one.

2. CCMD -2: Honor Thy Data

Information is the life blood of today's digital economy. It's hard to think of any business that could survive today without it, so it's important to understand what data your business needs to function efficiently. **Know your data. Know what's important. Know what you are collecting. Know where it flows. Know who it belongs to, and who has access to it from which devices. Know how it is processed and stored. Know when it is in use, at rest, or in transit. Know what laws, contractual obligations, industry guidelines, and regulations govern it based on the type of data it is and where it originates or is stored geographically.**

Every business has critical information that needs to be protected for business continuity purposes. Information such as: trade secrets; lists of clients and their contact information, revenues, costs, solutions, contracts, legal concerns, account plans; supplier information like manufacture bill of materials, costs, terms and conditions, production schedules; research & development IPR; financial

[14] See footnote 2
[15] See footnote 7

performance indicators; corporate M&A activities; operational business plans; network diagrams; application and software inventories; system configuration information; employee personal data; insurance policies; healthcare information; business strategy; pending litigation efforts; product pricing, margins, and marketing campaigns; and competitive and internal SWOT analyses are some of the items that are most important. Some of these types of data are regulated while others are contractually protected by legal agreements with clients, suppliers, and partners. The rest is probably too important to your business to treat haphazardly.

Recommended Actions

Work with business data owners to identify, categorize, and classify important business data. Prioritize how to protect and defend your data based on how critical it is to your business, and based on the desired degree of compliance with laws, regulations, and industry guidelines that your risk appetite dictates. Not all data is created equal so resist taking a broad brush approach and treating all data exactly the same with the same prioritization and controls. Spend the most time, money, and resources on the most critical data for your business to ensure the cost benefit analysis makes sense. Minimize the amount and types of sensitive data that you collect, use, share, and store. Isolate it to properly segmented parts of the network to reduce scope of compliance requirements and to narrow attack surfaces. Restrict data access to authorized resources and devices only. Monitor all modifications to ensure data integrity. Create, implement, and continuously reinforce a data security policy for your organization that outlines expectations on securing business data with tangible consequences for failing to do so. Adopt a **data centric, identity dependent, real time, zero trust security** philosophy. What does that mean? It means regardless of device or where a resource may be physically located, the degree of data protection should be dependent on the sensitivity classification level of the data, should have strong authentication and identity management procedures to restrict access, should operate in real time with alerting and rapid response capabilities, and should never assume the "goodness" of any traffic or resource.

3. CCMD-3: Thou Shalt Know Thy Threat Landscape

Never has it been more important to understand the potential threats, attack vectors, and hostile agents that lurk in cyberspace than today. There is no shortage of annual security reports that cover the breadth of the threat intelligence arena and/or focus on particular verticals. Numerous well respected vendors, service providers, research organizations, academic entities, and governmental bodies publish insightful threat and breach reports. Business owners of all sizes need to have at least a high level awareness and understanding of the threat landscape in which they operate in order to better understand their cyber risk landscape.

I recommend the annual ENISA Threat Landscape report as a good starting point. ENISA stands for the European Union Agency for Network and Information Security organization and its publications can be found at www.enisa.europa.eu. They do a good job of describing the threat environment

sufficiently without diving too deep into the technical minutia. As an example, their *Figure 20: Overview of Agents in Cyber Space* below from the ENISA Threat Landscape 2013 provides a great visual to help frame the players on the cyber agent roster. [16]

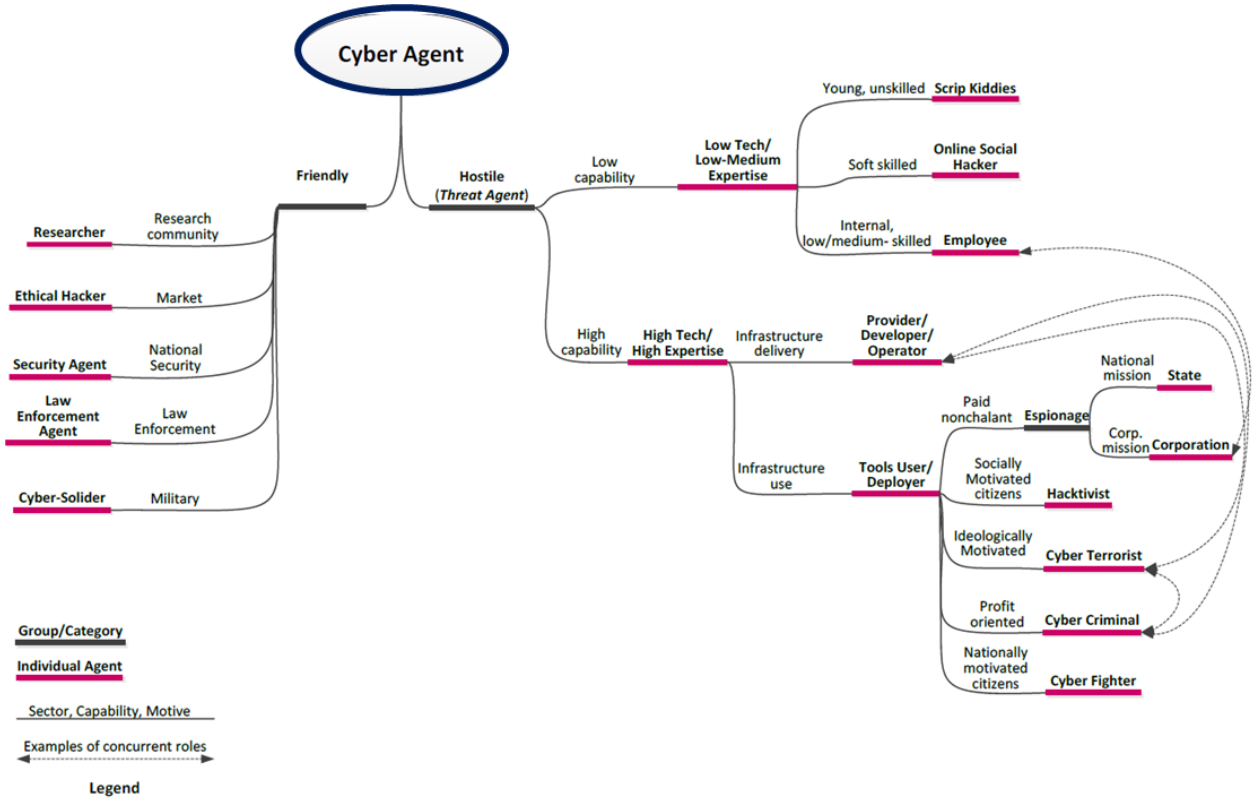

Figure 20: Overview of Agents in Cyber Space

Source: www.enisa.org

Business owners and executive stakeholders need to understand at a high level what risks these types of cyber agents may pose to their business goals.

They also need to have an appreciation for what type of threats exist that these agents have the potential to utilize. ENISA's annual threat Landscape 2014 report has a useful summary chart that at one glance can give a business owner an overview of what the past year's global threat landscape looked like and the general directional trends they have seen. [17] Each of the top threats is covered in more depth in the report and gives the reader a good general understanding of the nature and impact of the top threats.

[16] *ENISA Threat Landscape 2013 – Overview of current and emerging cyber-threats*. ENISA. (Dec. 2013) Retrieved from www.enisa.europa.eu Aug. 2015.
[17] *ENISA Threat Landscape 2014 – Overview of Current and Emerging Cyber-threats.* ENISA. (Dec. 2014) Retrieved from www.enisa.europa.eu Aug. 2015.

ENISA Threat Landscape 2014
Overview of current and emerging cyber-threats
December 2014

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014[1]

Source: www.enisa.org

Many of the annual threat and breach report providers also offer real time threat intelligence services that a corporation can incorporate into their overall security program. Real time threat intelligence information is invaluable in helping companies of all sizes to quickly pivot and respond to current cyber threats. Active utilization of real time threat intelligence is a data security best practice.

Lastly, business owners need to understand the value that a target device on their network potentially offers to a cyber threat agent. Brian Krebs, author of the *Krebs on Security Blog*, created the diagram below to help educate the public on the potential "nefarious uses" of a hacked personal computer. While consumer centric in nature, business owners need to think about how a similar

diagram might look if the "hacked PC" was replaced with a "hacked web/database/email server or corporate laptop."

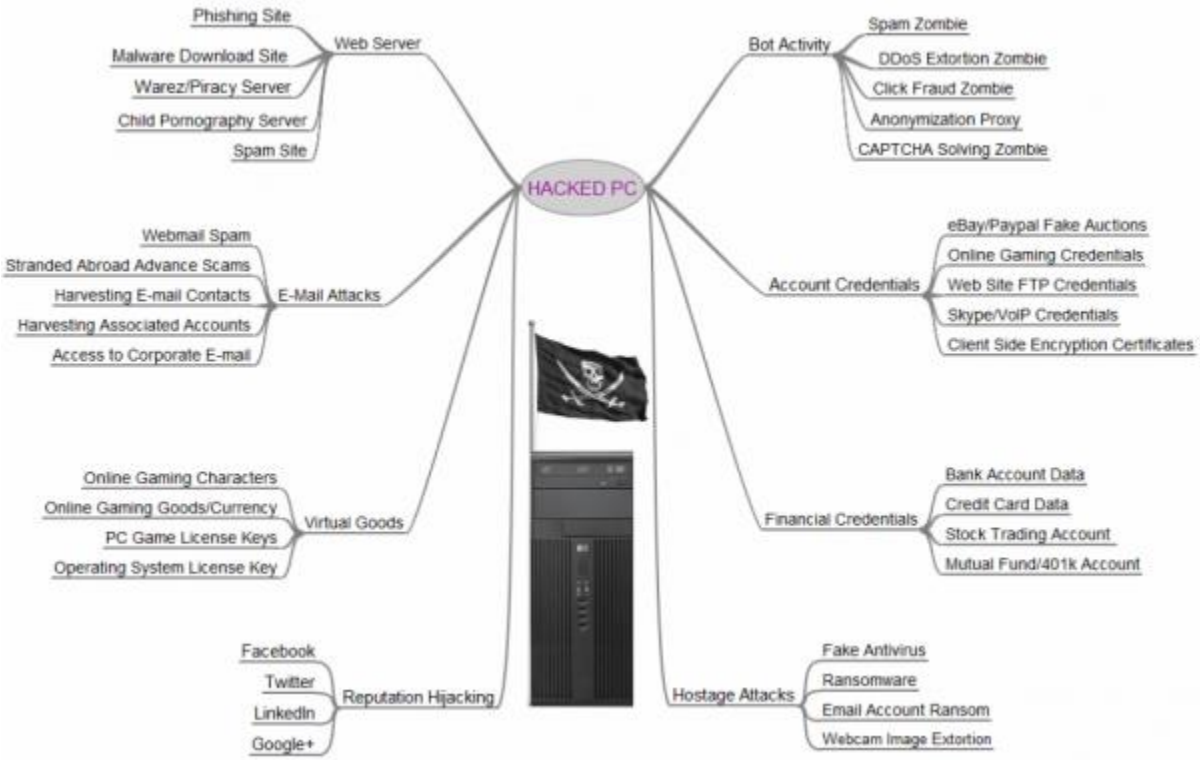

Figure 5: http:krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisted/ accessed August 4, 2015

Recommended Actions:

Having an adequate understanding of the environment around you is the first step in preparing to adapt to it successfully. Be aware of the types of black hat activities that are running rampant in the wilderness you operate within. Educate yourself. Start trying to think like a bad guy. Understand the threat landscape surrounding your business. Role play as each type of cyber threat agent. Think about what information you would go after within your business or your industry if you were one of them and why. Read threat reports to learn about the current cyberattack trends overall. Seek out the reports covering the threats that are most prevalent across your geography and your specific vertical. Understand where the vulnerabilities to these types of threats lie within your network. Determine which ones have high risk of occurrence based on potential value to the threat agents most likely to target a business similar to yours, and which ones have the biggest impact to your business operations if compromised. Ensure your security controls address them sufficiently.

Incorporate real time security threat intelligence into your security activities. There are numerous cloud security solutions available today that can provide this capability more cost effectively than ever before.

Information Sharing and Analysis Organizations (ISAO) are additional resources that can be used by businesses to better understand their threat environment. ISAOs collect, analyze, and communicate cyber threat intelligence to member organizations. Businesses may also consider joining relevant sector specific Information Sharing and Analysis Centers (ISAC). The National Council of ISACs (NCI) has a list of member industry ISACs that covers aviation through the water sector at http://www.isaccouncil.org.[18] There is also the recently formed Department of Homeland Security National Cybersecurity and Communications Integration Center (DHS NCCIC) whose mission is to provide 24X7 situational awareness and incident response support for the Federal Government, law enforcement, and intelligence communities while also sharing information with the private sector. [19]

4. CCMD-4: Remember Thy People & Honor Them with Education

People are both a business' strongest asset and their biggest potential security weak spot. As insiders, they bring inherent risk of intentional and inadvertent threats. The focus of this commandment is on inadvertent cyber risks that can be reduced through employee security awareness training. Other internal controls beyond awareness training are needed to address the risk of insider fraud and intentional insider cyberattacks.

Figure 6: Weakest link in security chain www.s2reb.com

Wombat Securities Technologies indicates that investments in security awareness training can reduce infections by as much as 45% to 70%.[20] Aberdeen Group analysis shows that by successfully changing end user behaviors through training, an organization may realize up to 60% reduction in user driven security risks.[21] With the latest Verizon research advising that people are the common factor across the top three breach attack patterns, it's critical for all businesses to better educate

[18] "Member ISACs." *National Council of ISACs*. WEB. Aug. 2015 <www.isaccouncil.org>
[19] "About the National Cybersecurity and Communications Integration Center Homeland Security." *Department of Homeland Security.* WEB. Aug. 2015 < www.dhs.gov>
[20] Brink, Derek. "The Last Mile in IT Security: Changing End User Behaviors" Wombat Security. (Oct. 2014) WEB. Aug. 2015 <www.wombatsecurity.com>
[21] Ibid.

and continuously increase employees' level of understanding and ownership with respect to good cyber hygiene practices. [22]

All employees come to work with a mixed bag of skills regarding technology, of respect for privacy, and of recognition of their role in keeping data secure. While there are many tech savvy and security conscious people, a large number are likely part of "The Great Digital Uninformed" (GDU)[23] who commit the Five Deadly Cyber Attitudinal Sins™ below.

The Five Deadly Cyber Attitudinal Sins™

1. Employees don't know what steps to take to keep their data and devices secure
2. Workforce doesn't understand which of their behaviors is risky or why
3. People don't think twice about sharing information personally or professionally
4. Resources don't realize how their personal digital habits impact their work environment
5. Nobody cares enough ***yet*** to do anything about it

The Five Deadly Cyber Attitudinal Sins™ are pretty much the harbingers of breach for any organization. An effective security awareness program can address all of these but it has to first address the personal apathy component in order to have a solid foundation to build on. Businesses have to incorporate personal relevance into their security awareness training to get employees' attention on what improving their data security skills means to them, and do so continuously for real change to take root. If they can take what they learn at work and immediately apply it every day in their personal lives as well, it will soon become an unconscious habit.

Recommended Actions:

Make cyber security awareness and training a continuous priority in your business. Start in the hiring process by discussing cyber habits with top candidates before extending job offers. Doing so puts them on notice that proper data handling behaviors are a job requirement. This is especially important for software developers, programmers, product designers, sales resources, and senior executives. For the first three roles especially, a deeper dive during the interview process looking at their cyber skill sets, secure development experiences, and design attitudes toward data security will only strengthen your R&D bench going forward and reduce future development costs. Your sales resources are hardened road warriors, and are one of the most likely functions to need valuable data constantly while on the go. Discussing BYOD, social media use expectations, and proper safeguarding of confidential client and company information upfront sets the stage for security success. Making sure your future executive team walks the data security "walk" and not just mouths the "talk" will ensure the proper tone at the top. Avoid hiring the "Hillary Clinton" senior executive who thinks it's acceptable to use their personal email account and server to conduct day

[22] 2015 Data Breach Investigations Report. *Verizon*. Retrieved from www.verizonenterprise.com. July 2015.
[23] Gelbstein, Ed. "Imperfect Technologies and Digital Hygiene: Staying Secure in Cyberspace." *ISACA Journal.* (2014). WEB. Mar. 2015 <http://www.isaca.org/journal/archives/2014>

to day business operations. Your security policy and acceptable use agreements should apply equally to all employees regardless of rank. The sooner you set that expectation within the senior ranks, the faster you will start to see a security conscious culture grow across the organization. Make sure your executive team leads securely by setting the example.

Include initial basic cyber hygiene training as part of the employee onboarding and ramp materials. Tailor ongoing quarterly training to specific role based content, company security trends, and the business regulatory environment for each major job function to help them understand how their digital actions directly impact strategic business objectives. Avoid making it a compliance "check the box" type of activity. Treat it like a new product launch and invest marketing dollars to "brand cyber security" internally. Set up a rewards program for employees adopting best practices. Show them how to secure their personal lives for desired behaviors that impact their professional ones. Ensure data security policies and acceptable use agreements have some teeth in them for non-compliance, and are reviewed and acknowledged in writing at least annually.

5. CCMD-5: Thou Shalt Know Thy Network

TECHNOLOGY WARNING! Before you bolt, remember that it has taken to the fifth commandment to start talking about technology at any level of depth or pain. It's a huge understatement to say that today's business networks can be complex. They can vary from the micro business with a residential grade wireless broadband router hanging off a cable or DSL modem at their SOHO business to an intricate, globally distributed, state of the art, fully redundant, F100 mesh topology network with tens of millions of dollars invested in equipment. This is where most business owners check out with glossy eyes and hand it over to the IT folks to tackle. That is totally understandable when getting into the weeds of a network but remember that you cannot outsource the business ownership and strategic responsibility of data security to either the internal IT team or to an external third party. You can only outsource some of the tactical implementation and operational services associated with it. Overall responsibility remains with senior business leaders.

Regardless of size or complexity, you still need to know the same information in order to safeguard your network to the fullest extent possible. You need to:

- Know the overall physical and logical layout of the network
- Know the authorized applications, devices, and data flows that ride over the network
- Know all entry and exit points
- Have an inventory of all authorized nodes and devices on the network, their connection points, and identify any shared or virtualized infrastructure

- Determine where all network nodes carrying business data geographically reside and who has physical ownership and legal responsibility for any non-company owned infrastructure your network utilizes (PaaS, IaaS, or traditional hosting)

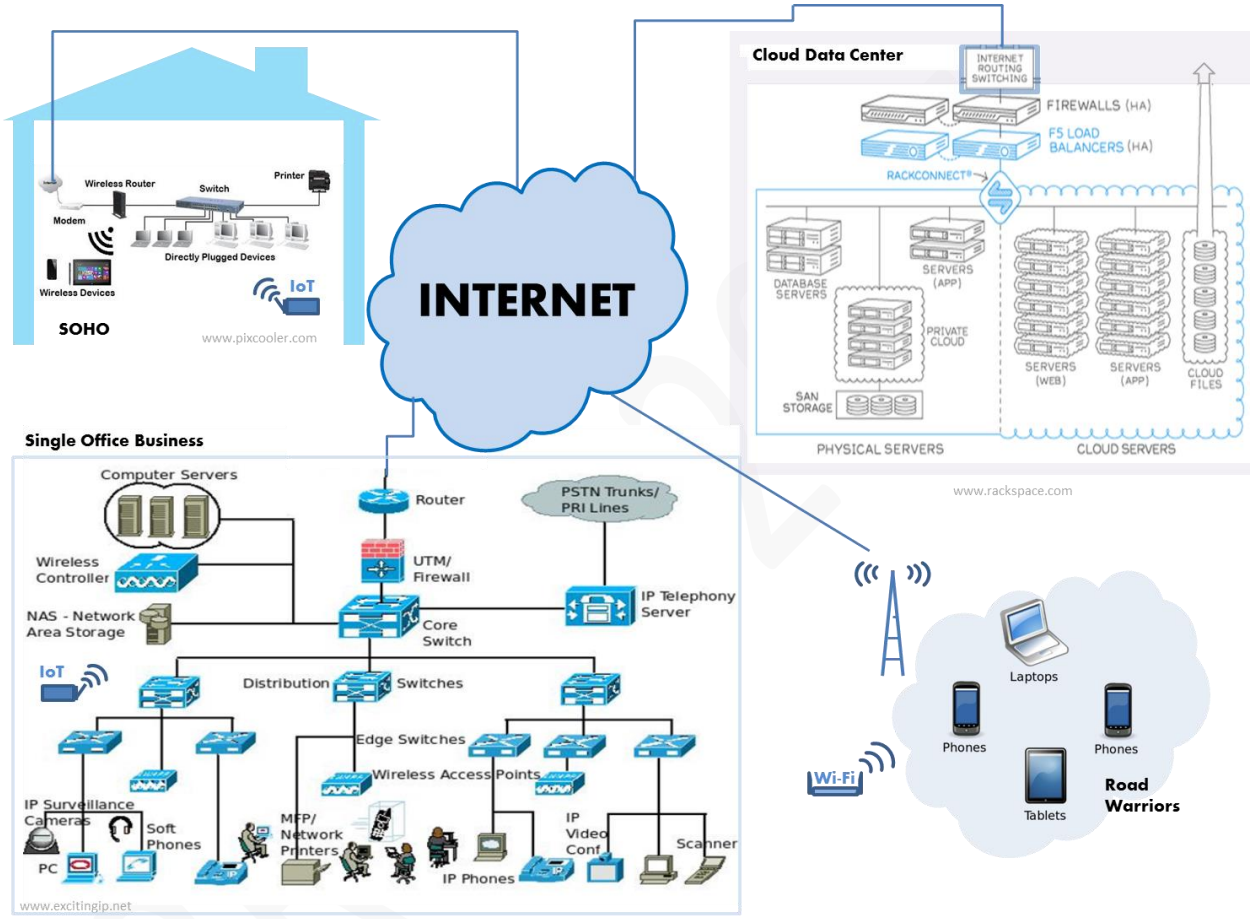

Figure 7: Typical SMB Network

- Have a clear picture of what exposure points your network may have given the physical and logical access and interconnection points
- Make a special effort to identify how BANs (Body Area Network – think Fitbit®), Internet of Things (IoT), machine-to-machine (M2M), and any industrial control systems (ICS) are connected
- Understand the overall security pros and cons plus recommended controls for each type of network solution you have deployed
- Know BIOS, firmware, hardware, and software versions; unique equipment identifiers; vendor contact information plus their product update/patch/security notification policies

and your communications escalation path for all gear deployed within your network infrastructure

- Establish, document, maintain, log, and monitor standard operating and security configurations for all your gear; alert on configuration changes
- Know all protocols and services that are running over your network
- Know where technical security controls are implemented within the network regardless of whether it's your own network or a third parties' network, and who has access and authorization to modify those controls
- Have an accurate network diagram plus track and restrict access to it
- Have strong network change management policies and procedures
- Restrict logical and physical network access
- Minimize and tightly monitor remote access privileges especially from third parties
- Isolate sensitive data from the mainstream internal network and routinely conduct network penetration testing to verify proper network segmentation and data isolation
- Conduct background checks on all employees and third party resources that have physical and logical access to the network
- Close all non-used logical ports on network equipment
- Monitor continuously with real time logging, alerting, and response
- **DEFINE YOUR NETWORK NORMAL**

Notice that most of the above are "inventory" or "mapping" in nature meaning you need to document and closely monitor everything that is in and rides over your network inclusive of who has access to the network. Networks are dynamic beasts so documenting and controlling changes to them is part of the change management process challenge you need to adopt. Your network was built to connect you to what you need to conduct business effectively so you should know what services, applications, external IP destinations, protocols, transmission patterns, and geographies are legitimate. That is why the last bullet regarding defining your network normal is bolded. Once your network normal is defined and understood, it is easier to identify anomalies that warrant further investigation as those anomalies become potential network indicators of compromise (IOC).

Recommended Actions:

Rome was not built in a day so if you have not already fainted from reading the list, then there is still hope for you! Breakdown securing this information into prioritized, bite sized blocks that your network team can tackle over a reasonable period of time. Your network team could be your own IT resource, somebody on staff who tinkers enough with technology to be your informal IT guy, or a technology service provider (telecom company, reseller, IT contract firm, consultant, etc.) that you already work with. They do need to have sufficient skills and/or access to tools to handle all of the above. This is where automated network and asset discovery tools will make these tasks much easier and increase accuracy and relevance. Bits and pieces of this information likely already exist but are scattered around and not formally documented from a system wide network view. Start

with figuring out what you have readily available. Update it with the information that is easiest to get your hands on. Work closely with your network team to secure as much of this information as makes sense to do in phases. Hold them accountable for safeguarding your network information whether your "network team" is internal or external. This type of network information is mission critical so strong internal access controls and vendor management practices are required to ensure adherence to your company's security requirements. Whoever is doing your network design, implementation, and maintenance needs to be fully vetted from both a background check perspective and from a qualifications perspective as your network is your kingdom, and it must be guarded relentlessly. Remember that networks are constantly changing so diligent monitoring combined with documenting and controlling modifications to them is part of the security challenge you need to adopt as well.

If you utilize IaaS in your network, do your due diligence on the cloud provider to ensure adoption of the Cloud Security Alliance's (CSA) guidance on cloud security focus areas [24] and their implementation of the recommended controls outlined in the CSA's Cloud Controls Matrix.[25] Make certain your IaaS provider has a security program and culture that aligns with yours. Another key service provider certification to look for in your cloud provider is a Service Organization Controls (SOC) 2 Type II report. (http://www.aicpa.org/soc) Request a copy from your provider and review the effectiveness of their controls against all five Trust Services Principles.

For critical infrastructure companies, defense oriented firms, companies with ICS, and for other highly sensitive corporate data, take the time to understand the nuances of your network infrastructure vendors' supply chains. Do the deep dive right down to the manufacturer(s) of the chipsets and circuit boards used plus understand the secure development practices of their firmware and OS providers. Also remember to think outside the traditional network box and consider potential attack vectors coming from wireless (near and far field)/wireline power transmissions that enable broadband over power delivery IF your risk environment warrants it. A word of caution here – Be diligent but manage your paranoia level to what best fits your risk environment AND proves in via a cost benefit analysis.

Think carefully before sharing or publishing network information externally. Use caution when participating in vendor case studies or whitepapers about your network configuration and equipment choices as that information may be used in early reconnaissance activities associated with advanced persistent threats (APT).

Follow that same advice for network related job postings. While you need to share enough information to attract the right type of skilled resources, avoid sharing any information in posted job requirements or during interviews that may highlight network technologies that have long

[24] "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0" *Cloud Security Alliance* (2011) WEB. Retrieved from www.cloudsecurityalliance.org. Aug. 2015

[25] "Cloud Controls Matrix v3.01 (CCMv3.01)" Cloud Security Alliance (2014) WEB. Retrieved from www.cloudsecurityalliance.org. Aug. 2015

standing vulnerabilities like a server that is no longer manufacturer supported with security software patches.

6. CCMD-6: Honor Thy Code

TECHNOLOGY WARNING! Software may be King in our application centric world but it's important to remember "Where there's an APP for that, there's a HACK for that!™" No code is ever completely secure nor is programming perfection required for good security. Just like network aware CCMD -5, Honor Thy Code is about taking an inventory of the software and its structural underpinnings that your business depends on. It's about looking at the system of software and applications across the enterprise, and their interaction with the underlying platforms, APIs, networks, databases, and libraries that they touch.

This commandment has two parts: purchased or commissioned software (software built by others for your internal use) and developed software (software built by you for your internal use and/or for others' commercial use.) If you purchase commercial off the shelf (COTS) software or pay third parties to develop custom business applications, you are focused on the purchased portion of CCMD-5 which is more about proper vendor/supplier management than it is about having an in-depth knowledge of how to design and deliver secure software. If you develop your own custom software or develop applications for purchase by others as COTS solutions, it's all about adopting secure software development practices.

For secure software (SW) development, your development team needs to:

- Design security in from the outset of and through the entire software development lifecycle (SDLC)
- Follow secure SW development best practices from recognized industry groups like NIST,[26] SAFECode.org,[27] and CERT.[28]
- For all application interactions (whether initiated by humans, system processes, or APIs) know and utilize the fundamentals of secure software design: protect information from disclosure, modification, and destruction; properly authenticate at all trust boundaries;

[26] Security Considerations in the System Development Life Cycle." *NIST Publication 800-64*. <http://csrc.nist.gov/publications/nistpubs/800-62-Rev2/SP800-64-Revision2.pdf>
[27] "Fundamental Practices for Secure Software Development 2nd Edition." *SAFECode*. <www.safecode.org/wp-content/uploads/2014/09SAFECode_Dev_Practices0211.pdf>
[28] "Top Ten Secure Coding Practices" *CERT Software Engineering Institute – Carnegie Mellon University*. <www.securecoding.cert.org>

ensure authorization; enable auditing; implement input and output validation; manage configurations, sessions, and exceptions effectively[29]

- For mobile apps, SaaS solutions, and traditional software make use of OWASP Top 10[30] and Common Weakness Enumeration[31] (CWE) along with other top SW vulnerability dictionaries and catalogs as applicable
- Implement encryption methodologies correctly, institute solid key management techniques, and carefully document encryption protocols and algorithms used
- Understand the production environment the SW will be used in and build appropriate threat models
- Make no assumptions about any other security controls in the production network or across the rest of the stack that application security will depend on – BUILD SOFTWARE STANDALONE SECURE
- Use Common Attack Pattern Enumeration and Classification[32] (CAPEC) to identify and understand possible attacks to utilize in threat modeling activities
- Know the Common Vulnerabilities and Exposures (CVE)[33] associated with your development environment and their Common Vulnerability Scoring System (CVSS)[34] scores
- Create data flow diagrams covering end to end application use scenarios to identify high risk input and output areas
- Understand data classification and protection mechanisms required for sensitive data handling within applications
- Regardless of programming language check input validation against proper character set, length, and data format expected; escape all special characters; sanitize data to filter out dangerous characters[35]
- Understand the business, legal, and regulatory environment the software will likely operate within and ensure compliant design
- Validate SW security controls with static, dynamic, and fuzz testing; optimize testing automation
- Understand the overall Identity, Entitlement, and Asset Management process for application usage and data access within the production environment
- Conduct vulnerability assessments and penetration testing of software in pre-production and production environments
- Document, review, and understand functionality of all open source code, libraries, databases, utilities, APIs, reused code, etc. that are components of the software

[29] See footnote 27
[30] "OWASP Top 10 - 2013." *OWASP.* (June 2013) WEB. Aug. 2015 <www.owasp.org>
[31] "CWE Version 2.8." MITRE. WEB. Aug. 2015 <www.cwe.mitre.org>
[32] "CAPEC Dictionary." MITRE. WEB. Aug. 2015 <www.capec.mitre.org>
[33] "CVE List Master Copy." MITRE. WEB. Aug. 2015 www.cve.mitre.org or National Vulnerability Database <www.web.nvd.nist.gov>
[34] "CVSS v3.0." FIRST. WEB. Aug. 2015 <www.first.org>
[35] "Website Security 101." WhiteHat Security. (June 2007) WEB. Aug. 2015. <www.whitehatsec.com>

- Know the data handling details for all APIs touching sensitive information
- Know and follow the vendor recommended secure design guidelines for specific platforms and languages being used in the development environment
- Evaluate code for both security and privacy risk exposures
- Know what data the application is collecting and abide by all applicable laws, regulations, disclosures, and required consents that govern its collection, storage, use, sharing, and destruction
- Train development teams on secure SDLC best practices and hold them accountable to deliver
- Hire certified secure software developers whenever possible
- Institute a software assurance program with a formal response process for addressing reported software vulnerabilities
    - Ensure you monitor for and receive notifications of any reported vulnerabilities in the open source code, libraries, databases, utilities, APIs, and reused code within your software
    - Establish a reported vulnerability review process to determine impact, corrective actions, and client communication strategy

If you purchase software from third parties, you need to:

- Hold them accountable for all of the above listed items with RFP and contractual language
- Ask for written proof of their software assurance practices and historical track record on security issues and response timeframes
- Validate secure coding independently to the extent you can via binary code analysis or other techniques without violating relevant EULAs (end user license agreements)
- Know software versions, vendor contact information plus their software update/patch/security notification policies inclusive of signed code validation methodologies, and your communications escalation path
- Ensure software vendor provides inventory of all open source code, libraries, databases, utilities, APIs, reused code, encryption protocols and algorithms used, etc. and any associated licenses that are components of the purchased software ; track for reported vulnerabilities
- Secure written commitments on vendor timelines to resolve any reported vulnerability [36] classified as CVSS Severity HIGH (CVSS base score range of 7 or higher [37])
- Ask about vendor's internal security posture and information security policies to gauge alignment with your company's approach
- Inquire as to their relationship with the security research community overall and how they respond to third party reported security vulnerabilities impacting their software

[36] National Vulnerability Database. NIST. WEB. <www.nvd.nist.gov>
[37] "CVSS v3.0." FIRST. WEB. Aug. 2015 <www.first.org>

- Inquire if they have a formal bug bounty program for security researchers to find and report security vulnerabilities directly to them and their time commitment on investigating and taking actions to resolve based on severity
- Ask about vendor secure software development industry certifications for vendor as a whole and for individual developers contracted for any custom designed SW
- Ensure software fully meets all industry specific compliance requirements that are relevant to your business; secure written vendor confirmation and objective third party verification of compliance where possible (i.e. PA-DSS, etc.)[38]
- Know how the applications and data flows interact with underlying network infrastructure and business processes/systems
- Determine where all applications carrying business data geographically reside and who has ownership and legal responsibility for any non-company owned applications (SaaS) or development platforms (PaaS) your business utilizes
- Create an applications and data flow diagram, and restrict access to it
- Establish, document, maintain, log, and monitor standard operating and security configurations for all your applications; alert on changes; incorporate Common Configuration Enumeration Project[39] information as appropriate
- Understand the overall security pros and cons plus recommended controls for each type of software solution you have deployed
- Monitor continuously with real time logging, alerting, and response for any code modifications

As you can see by the sheer number of important items listed above, secure software takes a dedicated team effort with a village of support. This commandment is simply too important to ignore.

Recommended Actions:

Document all software/applications in use within your business and rank by business impact. Focus on the most critical ones first and gather as much of this type of information as you can from the vendor or other publically available resources. Work it in manageable chunks until you have covered the applications that cover the majority of your business risks. Likely the 80/20 rule applies where just 20% of your applications will address 80% of your software related highest risks. The same guidance applies here as per the previous commandment, just change the word "network" to "software/applications" and follow the same "Recommend Actions" path inclusive of doing your due diligence on any PaaS or SaaS providers. Also remember that while investing in automated software testing tools adds immense value for this commandment, manual code review and adequate threat modeling upfront by security software engineers remains critically important.

[38] "PA-DSS Version 3.1" PCI Security Standards Council. (June 2015) WEB. Aug. 2015 <www.pcisecuritystandards.org>
[39] National Vulnerability Database. NIST. WEB. <www.nvd.nist.gov/cce>

7. CCMD-7: Remember to Keep Thy Network, Devices, Apps, & OS's Patched, Updated, and Holy

As a reward for persevering this far, this commandment is more about establishing processes with controls plus deploying sound change management to leverage the inventory work from the previous commandments then it is a nosebleed technical discussion. You have invested a lot of time and money acquiring software solutions, devices, network infrastructure and/or similar XaaS services. (XaaS where X=Infrastructure, Platform, or Software) You need to make sure that you take good care of them and keep them up to date.

Recommended Actions:

In general, follow the vendor's recommended use guidelines and maintenance schedules. Pay attention to product notices, quality alerts, security flashes, patches, and updates. Sign up for auto notification from the vendor for these types of events but don't necessarily implement blind auto updates or patches. Instead, establish a timely patch/update management process that works for your business. Validate any software updates are signed by legitimate vendor sources. Prioritize security patches. Maintain a test environment that mirrors your production environment to thoroughly test patches, updates, and configuration changes before production deployment to minimize costly disruptions. It's usually a good idea to stay within N-2 releases of any hardware or software solution to ensure manufacturer support is available. (N = current release) Avoid staying on legacy infrastructure or software that is no longer manufacturer supported as security patches are no longer being addressed. If a critical business function is dependent on gear or software that is no longer manufacturer supported, you need to secure some type of temporary emergency support capability and implement compensating controls for new vulnerabilities while you start the process to move off of the legacy gear or software as quickly as you can.

This is an area where adopting "anything as a service" (XaaS) solutions shine. The XaaS provider shoulders the brunt of this work and expense for the components under contract. However, as a customer you need to do your due diligence with the XaaS provider and understand: their data security policies overall; their procedures for infrastructure and application refresh, patch management and solution updates; and understand how their practices will impact your utilization of the service and your own security posture. Make sure you know where you have access and ownership for any security related items. Just like in CCMD-5 and CCMD-6, you need to ensure their adherence to the Cloud Security Alliance's (CSA) guidance on cloud security focus areas [40]and their implementation of the recommended controls outlined in the CSA's Cloud Controls Matrix.[41] Request and review a SOC 2 Type II report if available.

[40] "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0" *Cloud Security Alliance* (2011) WEB. Retrieved from www.cloudsecurityalliance.org. Aug. 2015

[41] "Cloud Controls Matrix v3.01 (CCMv3.01)" Cloud Security Alliance (2014) WEB. Retrieved from www.cloudsecurityalliance.org. Aug. 2015

8. CCMD-8: Thou Shalt Trust Only What is Known to be True

Earlier I mentioned how important it is to know your network normal, and its legitimate system interactions and data flows. The goal with this commandment is to allow only traffic and data exchange between known and sanctioned networks, nodes, devices, users, services, applications, and systems. Everything else should be blocked by default. This type of approach is known as whitelisting. Blocking only what is known to be dangerous and allowing everything else is known as blacklisting. Blacklisting requires that your "cyber crystal ball" is perfect and that you know in advance what malicious data may be coming your way. This is never the case for any new threat. Whitelisting is a much better approach when you are operating within a dynamically changing threat environment because it allows only pre-approved interactions to take place by default and blocks everything else.

Recommended Actions:

Implement a whitelisting approach within your technology systems to the extent possible. Blacklist where it makes sense to do so (i.e. anti-virus/anti-malware) but don't rely on blacklisting to keep any new threats out of your network. Gather your team and think hard about what "should be" your network and application "normal." Validate your assumptions with a baseline network and application "in use" test. Compare it to the initial assumptions. Investigate to understand and address any gaps. Repeat on a regular basis. Monitor regularly with real time alerts so you can respond whenever abnormal activity is spotted.

9. CCMD-9: Thou Shalt Adopt a Least Privilege Approach to Data and User Rights

CCMD-2 was about honoring your business data. CCMD-9 is about restricting who can access that honored data based on a "Needs to Know plus Needs to Use" access control approach.

Classification of data by sensitivity and value to the business was part of CCMD-2. Access controls address who is allowed to access each classification category of data. A good practice here is to use a Role Based Access Control (RBAC) methodology which ties data access to only the job functions that need to access the data in order to perform their roles.

This commandment also addresses the issue of restricting Super User and Administrative level of privileges. All users should be given the lowest possible level of system rights that is required to do their jobs. Additionally, anyone with Administrative level privileges should have another system user id account that they use for the majority of their day to day work that does not require the higher level of privilege to carry out their functions. They should only use their Administrative credentials when they are actually performing system administrative tasks. Adopting a least privilege approach applies equally to any intra/inter-system processes or APIs that require data access.

Recommended Actions:

Implement a RBAC and least privilege approach to data access as soon as you can. Ensure user's access rights are revisited frequently and make it mandatory to review access and privilege rights every time they change roles to make sure they don't continue to have access to data that is not appropriate for their current role. It should go without saying that Administrative accounts should NEVER be shared. Issue them sparingly and on a specific individual basis for personal accountability and appropriate use monitoring. It should also go without saying that you need to implement immediate removal of all access rights for terminated employees regardless of the circumstances of their departure. Even resources that have left on good terms need to have their access rights revoked promptly upon their exit. Logging, alerting, and monitoring safeguards should be in place to capture all unauthorized access attempts and unusual access requests from authorized resources.

10. CCMD-10: Remember Thy Connected Systems, Processes, and Business Interactions

No business today is an island. Even the smallest companies interact electronically with business partners, suppliers, service providers, and other external entities on a regular basis. The Rings of Cyber Relationship Risk™ from CCMD-1 shows the breadth of the type of business interactions that routinely expose a company to threats. These connected cyber relationships form a company's Ecosystem of Insecurity™. As shown in Figure 8, this interconnected business arena reinforces the importance of sound Vendor and Business Partner management policies, and the need for alignment of security philosophies and procedures between connected companies. It's critical to manage data security practices across the business ecosystem and to have a deep understanding of how each company's systems and processes interact with other parties based on the degree of integration, the type of sensitive information being shared, and of the relative "target value" of each company in the mix.

Figure 8 illustrates typical attack vectors used by cyber agents. Much like current flow, hackers will pursue the path of least resistance. The shortest path to ground for hackers is directly attacking a target company's staff and network resources. If those prove daunting, a company within one hop of the target company is the next viable option. First hop firms (within one hop) from high value F500 targets can be especially attractive to hackers if they are much smaller and not likely to have an army of security professionals on staff operating a fortress of security technology. Second hop firms require more finesse for a hacker to pull off but are still possible attack vectors for adept cyber criminals and some APT (advanced persistent threat) players. Even third hop firms may come into play for nation state sponsored APTs.

Recommended Actions:

Understand your Rings of Cyber Relationship Risk™. Take the insights gained from CCMD-1, CCMD -2, CCMD-3, CCMD-5, and CCMD-6 and prioritize which Business Interactions are mission critical for the business. Shore up those relationships with strong vendor management procedures, contractual data security practices, and validate security alignment. Take a hard look at your business as a whole from an interconnected system wide perspective to understand how each process and handoff point can potentially impact the safe handling of sensitive data. Understand the risks identified from CCMD-1 and CCMD-3. Are you a high value target? Are you a first or second hop firm to a high value target? All businesses should routinely consider first hop firms as potential high risk exposure points. If you have identified your business as a likely high value target then extend your security focus to also include second hop firms. Businesses requiring military grade security for highly sensitive data should consider expanding their security due diligence to third hop firms.

If a major business partner is unwilling or unable to work together toward a shared security vision, consider finding a replacement business partner or provider.

Take a system wide view of how sensitive data flows within your connected business processes and between your business partner networks. Redesign processes and limit the exchange of sensitive data to reduce potential leakage. Consider where it makes sense to encrypt sensitive data that is shared with external parties within your business ecosystem. Retain control in-house of encryption keys.

Think about your network, software, and devices supply chain as well as your connected business partners' supply chains. Are you comfortable with your sensitive data riding over their networks, through their devices, and being utilized by their applications IF their security requirement for their own supply chains are not aligned with yours?

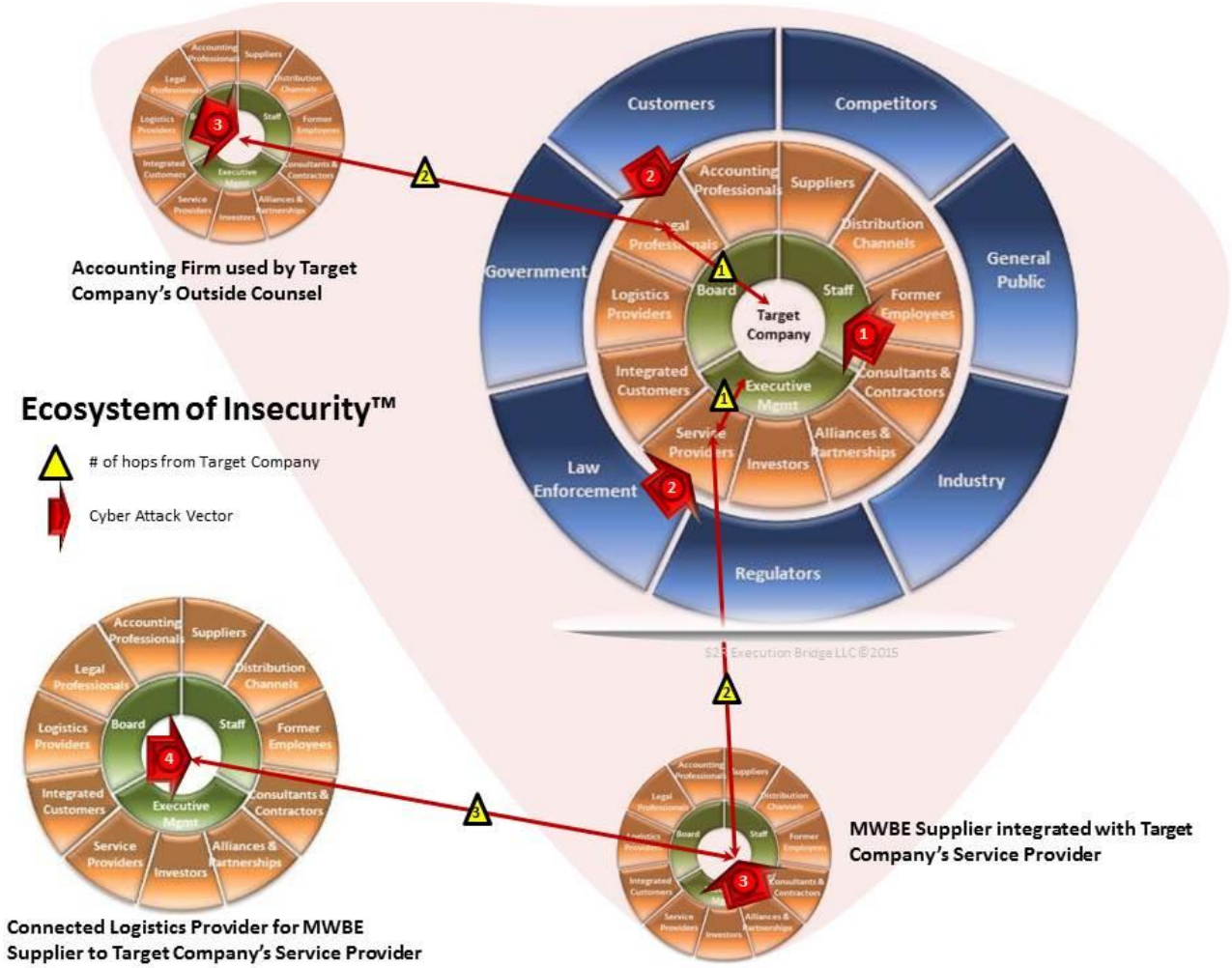

Figure 8: Ecosystem of Insecurity™ www.s2reb.com

11. Thou Shalt Balance Prevention, Detection, Response, & Recovery Investments

A breach at some level is pretty much inevitable for every business regardless of how much effort is put into prevention. The key is to make sure any breach you experience can be recovered from quickly with minimal impact to the business. To be able to hit that goal, you need to plan for a breach and how to respond just like you plan for disaster recovery and business continuity purposes. Doing so means you have to split your focus across prevention, detection, response, and recovery activities in order to be prepared. The faster your security controls can detect an intrusion, the faster your response efforts can tackle the situation and restore system and network confidence through their recovery efforts.

Recommended Actions:

Avoid putting all of your security eggs into the prevention basket. You need to expect the cyber fox to eventually break into the data hen house so plan for the likelihood of a breach. Take precautions like encrypting sensitive data where it makes sense to do so. Invest in detection capabilities that recognize intrusions in a real time fashion. Ideally those detection capabilities also have the ability to automate containment activities in addition to alerting on the security event. Create an incident response plan to address likely breach scenarios and train responders thoroughly on the plan. Test the plan on a regular basis to keep it fresh and relevant.

Establish relationships and support agreements ahead of time with the type of resources you will need to respond and recover effectively. If you don't have in-house capabilities for cyber incident response, you need to retain the services of technology service providers that offer those capabilities **before** an incident so you have the luxury of time to evaluate candidates and negotiate pricing without cyber fires running amok in your systems. Reach out before you need their help and establish contact with law enforcement resources that handle cybercrimes and understand each organization's cyber role and responsibilities and what information they will need from you to assist in the response. Know how the FBI, Secret Service, or state and local law enforcement can assist you and how to engage them. Consult with your attorney for guidance on when to notify general counsel of a security incident. Make sure they have reviewed and approved of your incident response plan especially its communications strategy and forensic evidence preservation efforts.

For those business that don't have their own information security resources or even general IT staff, this is an area where evaluating a managed security and incident response service offering is worth the effort.

12. Keep Sacred the CIS Critical Security Controls [42]

TECHNOLOGY WARNING! With so many things to think about for data security, organizations often hesitate in taking actions due to uncertainty on what they should do first that will offer them the highest and fastest returns for their security investments. The Center for Internet Security (CIS) maintains one of the best resources available to help companies of all sizes cut through that uncertainty with "The CIS Critical Security Controls for Effective Cyber Defense." Designed to emphasize the "MUST DO" actions to improve security, it offers guidance to businesses on the top recommended security controls to implement for an immediate, high-value payoff.

[42] *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*. Center for Internet Security. Oct. 2015 Retrieved from <www.cisecurity.org>

The CIS Critical Security Controls[43] are:

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

CSC 1 through CSC 5 controls are called "Foundational Cyber Hygiene" by the Center for Internet Security and are considered essentials for security success. Their adoption should be prioritized.

For an even more focused starting point, the former Council on Cybersecurity (COC) used to have the "First Five Quick Wins." They were sub-controls that were deemed to "have the most immediate impact on preventing attacks." Interestingly, the latest iteration of the CIS Critical Security Controls from the now combined CIS and COC no longer defines "quick win" categories.

The old First Five Quick Wins were:[44]

1. Application whitelisting (found in CSC 2 and CCMD-8)
2. Use of standard, secure system configurations (found in CSC 3, CCMD-5, and CCMD-6);
3. Patch application software within 48 hours (found in CSC 4 and CCMD-7);

[43] Ibid.
[44] *The Critical Security Controls for Effective Cyber Defense Version 5.0*. Council on CyberSecurity. July 2015 Retrieved from <www.sans.org>

4. Patch system software within 48 hours (found in CSC 4 and CCMD-7); and
5. Reduced number of users with administrative privileges (found in CSC 5 and CCMD-9).

These items map closely to the Australian Signals Directorate's (ASD) "Top Four Strategies to Mitigate Targeted Intrusions" [45] which the ASD assesses will address "at least 85% of the intrusion techniques" to which they typically respond. If adoption of four to five fundamental tenets can reduce known intrusion risks by that much, they are definitely worth any organization's time and attention to implement swiftly regardless of their removal from a "quick win" formal categorization. Note again that only one of them involves a depth of technical skills - #2 use of standard security configurations. The rest are business environment, inventory, and process management related within an overall risk management framework that may require technical operational resources to implement if not automated in some fashion.

Recommended Actions:

Work with your internal IT resources, data business owners, and/or technology service providers to implement the old "First Five Quick Wins", CSC 1 through CSC 5, and CSC 12 as quickly as possible. Craft a phased implementation approach for adoption of the rest of the CIS Critical Security Controls. Guard against declaring victory after implementing the old "First Five Quick Wins", CSC 1 through CSC 5, and CSC 12. Without the added value of a corporate wide, data security risk assessment and formal, information security program to augment their technical implementation efforts, a firm can fall into a dangerous state of security technical complacency. Commit to moving from an ad-hoc Basic Cyber Hygiene & Compliance posture to a Defined Cyber Security Model per Figure 9.

Recognize that cyber risk is just one part of an overall information security and risk management (ISRM) program. All data regardless of whether it is in physical form, electronic form, verbal form, or is an abstract idea or knowledge held within employees' minds require the appropriate degree of protection based on its importance to the business. As your data security maturity level evolves, work to move beyond focusing on cyber risks and institute an overall information security risk management framework and governance framework gradually until your organization reaches a Managed Information Security Risk Management (ISRM) Program state.

[45] "Top 4 Strategies to Mitigate Targeted Cyber Intrusions." *Australian Signals Directorate*. (July 2013) WEB. Aug. 2015 <http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>

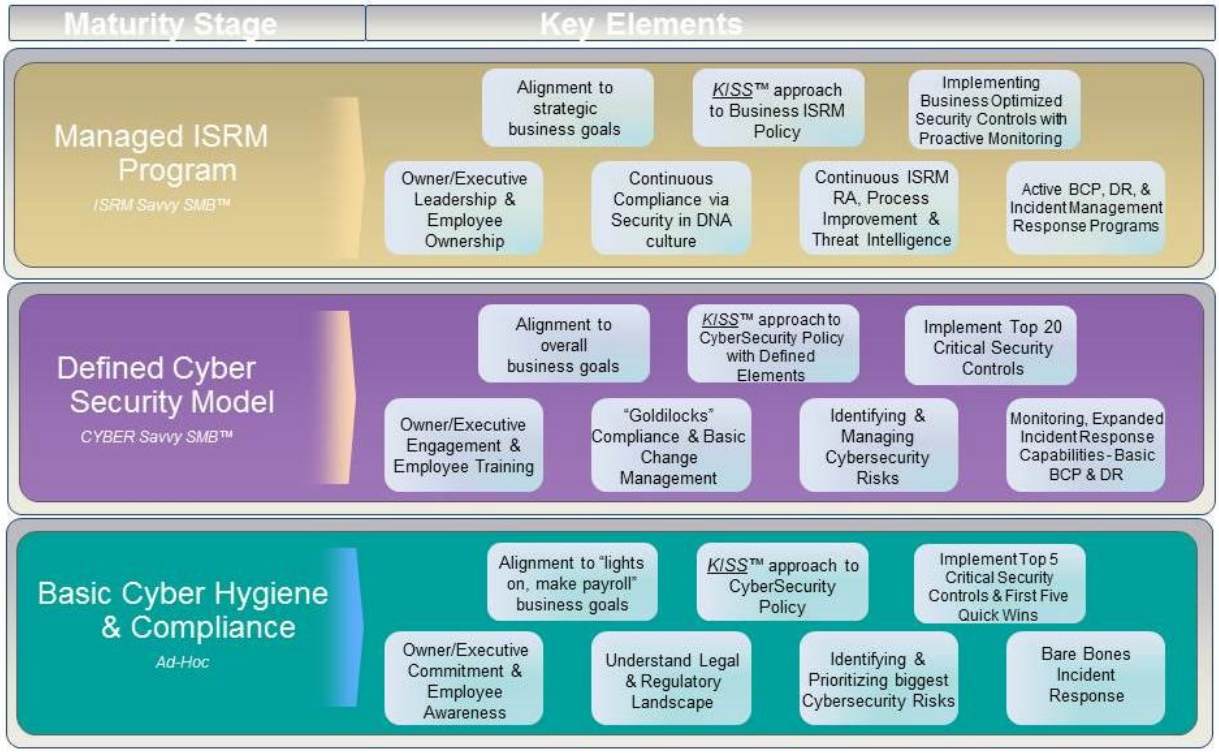

Figure 9: Data Security Maturity Stages www.s2reb.com

Conclusion

Data security is of critical importance in our information centric world. Cyber risk is a given in today's hyper connected business world. All companies that are connected to the Internet and using digital resources (computers, networks, mobile devices, electronic sensors, software, etc.) of any kind have an underlying and unavoidable cyber risk factor. Accordingly, every business needs to start the journey on shoring up their cyber security defenses and raising their situational awareness according to their threat environment and risk appetite.

A good place to start is for business owners and key stakeholders to discuss the SMB Data Security Cyber Commandments™ with their existing team of trusted advisors. Most businesses already have working relationships with technology service providers, lawyers, accountants, merchant bankers, and financial services advisors that can be leveraged to help them access the cyber risks for their business and to start the process of implementing a data security program that is a good fit for them. Consider complimenting those advisors with data security risk management professionals where needed to ensure a comprehensive risk assessment is shaping the security program development, written policies and procedures, and associated controls.

Don't get overwhelmed by the sheer volume of items that need to be addressed that you fail to start at all. Tackle it in prioritized steps based on a risk assessment and cost-benefit analysis. Develop a data security plan with a target implementation timeline. Adjust it as needed based on your business and threat environment. It's important to remember that data security is a marathon that requires commitment and constant attention. Tackle it in measured phases taking into account the highest risk factors, company culture and capabilities, and existing controls while moving to a more security conscious organization over the long haul.

The SMB Data Security Cyber Commandments reflect the intertwined nature of risk management, people, process and technology components that together build a secure and effective business system. Embracing them can guide your company toward reaching the optimal data security maturity stage appropriate for your business risk environment.

About the Author

Linda Hutchinson is President and Founder of S2R Execution Bridge, LLC – an information security risk management and business technology consulting company. The company specializes in helping small and medium sized firms craft business plans for profitable growth, develop multi-channel GTM strategies, evaluate their information security posture and governance practices, conduct risk assessments, and design security programs and policies while optimizing their technology investments.

Linda has over 15 years of experience as a corporate director at F500 technology companies in a variety of senior leadership roles spanning information communications technology, enterprise applications, and information security markets. She leverages her front line leadership experience in building international partnerships, restructuring turnaround businesses, and transforming sales organizations to deliver on the promise of bridging the gap between strategy and results, and closing the gap between technology and business objectives.

Ms. Hutchinson has a MBA from Emory University and a Bachelor of Electrical Engineering from Auburn University. Linda is currently a CISM® candidate having successfully passed the December 2014 exam. She is based in the Metro Atlanta area.

- Follow her online at www.s2reb.com
- Follow her on Twitter @S2REB_ATL
- Follow her on Facebook at www.facebook.com/S2RExecutionBridge.com

For licensing, reuse, and consultation services related to this whitepaper, please contact info@strategy2results-executionbridge.com