Closing the Cyber Security Risk Door

by Mark Trembacki

SUMMARY

Many current approaches to managing cyber security risk are reminiscent of the idiom, "shutting the barn door after the horses are gone." These approaches are not likely to be warmly embraced by shareholders, the corporate board of directors, executive management, or a company's customers because of the following:

- 60% of small companies are unable to sustain their business within six months of a cyber-attack. (House Small Business Subcommittee on Health and Technology, 2013)
- Major forecasters are predicting that a Fortune 1000 company will fail in 2017 as a result of a cyber breach. (Forrester, 2016)
- Data breaches are costly to a company's reputation and to the bottom line—and these two factors impact stock prices tremendously.

By taking the following three steps, companies can successfully close their cyber security risk door <u>before</u> incurring major data breaches:

1. ***Heed the basics***: 80% of cyber incidents can be avoided by deploying existing tools and practices.
2. ***Build resilience as well as prevention***: data breaches are a matter of when, not if, so having a plan ready to enact is crucial to a swift response and a successful recovery.
3. ***Leverage enterprise risk management (ERM) practices*** to handle cyber security management. Using existing processes is more efficient and effective as this approach covers all core decision and governance processes, thereby avoiding silos that result in unnecessary gaps.

STEP 1: HEED THE BASICS

The Commission on Enhancing National Cybersecurity recently reported:

> *"Many organizations and individuals still fail to do the basics. Malicious actors continue to benefit from organizations' and individuals' reluctance to prioritize basic cybersecurity activities and their indifference to cybersecurity practices. These failures to mitigate risk can and do allow malicious actors of any skill level to exploit some systems at will."* (Commission on Enhancing National Cybersecurity, 2016)

The 80% of avoidable cyber incidents stem from three sources:

A. Unintentional employee actions, including responding to phishing or social engineering schemes.
B. Vulnerable vendor systems, including inadequate data protection practices.
C. Unprotected or unencrypted portable devices like flash drives, laptops, etc.

Employee training, securing the practices of vendors, and encrypting laptops and portable storage devices are the basics that must be implemented in order to achieve strong cybersecurity practices.

From an organizational perspective, what do we mean by ***basics***? The following chart summarizes the basics that should be in place in <u>all</u> organizations, tailored as needed for the operating environment and size of the entity.

Category	Primary Actions
Policies and Data Prioritization	• Develop ***universal policies regarding cyber security*** covering topics including, but not limited to: acceptable use, e-mail, privacy, corporate mobility, social networking, data encryption (at rest and in transit), "BYOD" (Bring Your Own Device), physical security, and systems acquisition, development, and maintenance. • ***Prioritize the data requiring protection*** in order to risk-adjust the approach for mission-critical data ("crown jewels") such as intellectual property, proprietary information, personal information, or other legal requirements. • Articulate *risk appetite* and *risk tolerances* for IT security efforts.
IT Security Hygiene	• Install all ***patches, operating system upgrades,* and *other critical software releases*** to stay current with the best defenses against viruses, malware, and other online threats. • ***Protect all devices that connect to the Internet*** **-** computers, smartphones, tablets, and other web-enabled devices need to be protected from viruses and malware. • Use only ***company-issued encrypted USB flash drives and other external storage devices****,* which can otherwise be infected by viruses and malware, and use security software to scan them. • ***Develop effective access management*** **–** in addition to strong passwords, implement more advanced techniques like *multi-factor authentication* or *biometrics*. • ***Encrypt*** your most sensitive files, including data both at rest and in transit.
Primary Risk Sources: Employees and Vendors	• Develop an ***employee security awareness training*** program. • ***Implement employee monitoring*** (employee basics explored in more detail in the following section). • Deepen ***vendor management programs*** to include a cyber security filter in decision-making and monitoring processes for vendors. (see page 5).
Incident Response	• Create ***business continuity and incident response plans***. (see page 6). • Develop relationships with ***external experts*** to support recovery. • Explore the availability and cost of ***cyber insurance*** to reduce the impact of the financial and operating burden of a cyber incident.
Oversight and Monitoring	• Ensure cybersecurity is highlighted on ***management and board agendas***. • Develop ***timely, relevant,* and *understandable reporting*** for executive management and the board, including security intelligence, analytics, and dashboard type reporting. • ***Cultivate a strong cybersecurity culture*** through "tone from the top" to convey the strategic imperative of protecting data assets.

None of this is intended to shortchange the need for a strong technological defense. As attackers become more sophisticated, both offense and defense will continue to adopt the same innovations. Capabilities in machine learning, automation, and artificial intelligence can help address cyber security challenges. However, these more advanced tools are far more effective if the basics are firmly in place and operational.

Consideration should also be given to risk retention/transfer strategies. One byproduct of the increase in cyber incidents is the availability of a more robust set of data points to allow insurers to price and structure insurance products more accurately. As the market evolves, organizations need to assess the availability, coverage specifics, and cost of insurance as a mechanism to mitigate financial loss. That said, insurance is not a replacement for a comprehensive cybersecurity program. Similar to other risks, insurers will price according to an organization's cyber risk management and mitigation practices.

Insurers also provide another benefit to their clients by frequently having a pre-approved list of experts and advisors in place, such as attorneys, IT forensics specialists, communication consultants and others, to support recovery and remediation following a cyber incident. For companies without the requisite in-house expertise or existing relationship with firms offering these services, this benefit will make for a faster and more effective response in the important early days immediately following a cyber incident.

A: Employees → The First Line of Defense

90% of all cyber-attacks begin with a human weakness. (Martinez, 2014)

Cybersecurity is a human problem. Technologically-based defenses are needed to combat the ever-increasing sophistication of malicious threats. However, technology alone is not the answer. Consider these data points:

- In 2015, 60 percent of all attacks were carried out by insiders, either ones with malicious intent (45%) or those who served as inadvertent actors (15%) – in any case, they were people an organization would be likely to trust. (IBM, 2016)
- Ipswitch reported in a survey of more than 200 IT professionals and practitioners that a vast majority (84%) of the respondents send classified or confidential information as email attachments, often via personal e-mail accounts or free file-sharing services. (Ipswitch, 2013)
- According to the SANS Institute, 95% of all attacks on enterprise networks are the result of successful spear phishing in which a link in an email is used to execute an attack. (Brecht, 2015)
- In the results of over 8 million sanctioned phishing tests, 30% of phishing messages were opened by the target and 12% went on to click the malicious attachment or link. (Verizon, 2016)

Executive leadership must encourage cyber security management as more than just a routine compliance exercise. It is not a risk that can simply be delegated to the IT department. In the prior section, organizational basics were outlined; in this section, employee basics will be outlined.

Unintentional Employee Actions

When addressing the risks unintentionally posed by employees, the mitigation strategies may look like basic "blocking and tackling", but the pay-off in terms of risk reduction can be significant. Wombat Security Technologies and the Aberdeen Group found that "***an investment in user awareness and training effectively changes behavior and quantifiably reduces security-related risks by 45% to 70%***." (Wombat Security Technologies and the Aberdeen Group, 2015)

Employee education topics should include:

- **Authentication** - Set strong passwords, change them regularly, and don't share them with anyone. Employees should be required to change their passwords on a regular basis; automated reminders can be helpful.
- **Email links** - Links in emails, tweets, posts and online advertising are often how cybercriminals gain access. If something looks suspicious, even if the source appears to be legitimate, delete it.
- **Privacy and Social Media** - Limit the amount of personal information posted online, review privacy settings, establish safe browsing rules, and limit employee Internet usage in the workplace.
- **Social Engineering and Phishing** -Train your employees to recognize common cyber risks, including social engineering, online fraud, and phishing
- **Network connections** –- Public Wi-Fi, Bluetooth connections, and home networks are notoriously easy targets for hackers. Consider requiring a VPN connection or other remote access requirements.
- **Restricting user installation of applications** – Only approved software (to be used for business purposes) should be installed. Freeware (free games or software) and shareware are often sources of malware.
- **Backup** - Backup is the last line of defense against the permanent loss of data. In many cases, backup has saved not only days, but also months or years of someone's work.

In the broader context of protecting your data, physical security should also be incorporated into policies and awareness building with employees. Limiting and monitoring access (particularly to high risk/high value areas), discouraging tailgating (individual without access rights following an authorized user into a secure area), securing desktop computers, and implementing clean-desk practices all serve to enhance data security.

Employee engagement in awareness and training can be challenging. One simple yet powerful practice is to couple the company-focused cyber security awareness program with personal or at-home cyber security tips. Virtual reality and games that engage the employee in real life interesting situations can also be quite impactful in changing employee behavior. Educating employees on mobile devices, social media usage, and other topics of interest to them and their families will increase engagement while helping organizations achieve their internal cyber security awareness objectives.

Simply purchasing new technology won't increase the level of security. Employees need to understand their critical personal role in strong cyber hygiene and overall information management security.

Malicious Internal Employee Activities

Every type of organization is vulnerable to insider abuse, errors, or malicious attacks. These can impact reputation, operations, and profitability, and can expose data, harm the organization, or deliver valuable intellectual property into competitors' hands. Insiders can be current or former employees, contractors, or other business partners who have been granted authorized access to networks, systems, or data, and all of them can bypass security measures through legitimate means.

Relative to intentional activity, employees present additional challenges given they:

- May have extensive system knowledge.
- May have access credentials to sensitive parts of the system and data.
- Understand control mechanisms and, consequently, ways to avoid detection.
- Maintain the trust of the company.

Given the extent of internal intentional activity and damage that it can cause, organizations need to develop strong preventative and detective controls. These should be automated, as manual systems will not be sufficient. Mitigation strategies are less about culture and education and more heavily focused on preventing and detecting bad behavior.

In addition to the baseline of activities described in the prior section relative to employees, other measures to implement to mitigate malicious internal activity include:

- Conducting background screening on new employees, particularly those in sensitive positions relative to systems or data.
- Strengthening policies on access restrictions and auditing privileges.
- Ensuring proper restrictions are in place, and monitoring those restrictions rigorously.
- Limiting, monitoring, and controlling remote access and mobile device use.
- Addressing the challenge of external or temporary insiders such as consultants, support contractors, partners, service providers, and temporary employees.
- Monitoring and auditing the activities of general and privileged users, and quickly responding to any reported or suspicious behavior.
- Creating metrics to measure insider threat behavior and mitigation.

Although not unique to malicious activity, conducting regular penetration testing is necessary to evaluate security controls. Additionally, both physical and digital defenses are strongly needed to provide defense in depth.

The natural inclination is to trust employees, making the internal threat a formidable one. That said, if management has no visibility into the challenge, then oversight and governance will be extremely difficult.

B: Managing Vendors and External Parties

Third parties can be impactful to an operating environment:

> *"Boards and companies are not as attuned to cybersecurity risks for their third parties as they are for their own businesses, even though such issues can create the same adverse, long-term effects."* (The Shared Assessment Program and Protiviti, 2016)

Organizations that are laser-focused on delivering their missions through core competencies leverage the strengths of other providers and partners as a critical and viable business strategy. Companies manage hundreds, if not thousands, of vendor, third-party provider, and other types of outsourcing arrangements. These external parties are a primary source of incremental risk by creating new entry points into a company's technology environment. The sharing of data and communication is no longer fully in control of the organization, adding complexity and potential volatility to the operating environment.

Legal and other practical considerations can (and should) be employed to partition and mitigate the risk; however, the risk, no matter where it originates, will revert to the company in times of crisis or stress. ***Customers (corporate and individual) simply look to the company*** with which they are doing business for explanations and relief.

Many organizations are playing "catch-up" when it comes to vendor management. In a recent survey jointly conducted by Compliance Week and Crowe Horwath, 36 percent of respondents reported that identifying third-party relationships continued to be a challenge. (Jaeger, 2016) The ability to create a full inventory of vendor relationships is clearly "table stakes" in an overall program.

Like many business activities and models, the nature, size, and depth of a particular activity will strongly influence the type and sophistication level of risk and analytical tools in place. Outlined below are the basics for a third-party program as well as best practice attributes:

Ensure the basics. . . . .

- Inventory of all third-party contracts
- Third-party exposures prioritized on a risk-adjusted basis
- Assessment tools in place, including cyber impacts
- Vendor monitoring processes for adherence to contract provisions
- Actionable and timely reporting to senior management and the board
- Joint disaster recovery testing with primary service providers
- Technology-enabled vendor management solutions employed

. . . . . while aspiring to best practices

- Integrated with other processes – risk, procurement, etc.
- Enhanced inventory controls together with continuous monitoring
- Incorporating non-traditional "vendors" such as revenue sharing, joint marketing, referral agreements, joint ventures
- Developing internal change of use capabilities
- Fourth-party assessment and reporting capabilities to understand what activities have been further outsourced

For cyber security risk, "risk-adjusted" is no longer purely a dollar filter, i.e., based on the financial size of the contract. With the proliferation of inexpensive apps and other narrow, but highly effective tools, to fully capture the risk profile of the relationship, other filters must also be used to understand the impact to the organization.

An initial step entails the assessment of the maturity of an organization's overall third-party model as well as determining the way in which cyber risks are incorporated into the vendor management program. Third-party assessments of vendor practices may also be available through SOC (Service Organizational Control) 1, 2, or 3 reporting. These assurance reports provide strong insights into a vendor's control environment.

A strong third-party, vendor management program does more than strengthen cyber security risk management – it can support spending decisions, contracting strategies, service levels, and other critical operational activities to support the attainment of core business objectives.

C: Managing Devices

Stolen laptops remain an issue. As noted by Bitglass, *an organization is more likely to be robbed than hacked*. 68% of all healthcare data breaches since 2010 are due to device theft or loss, according to the 2014 Healthcare Breach Report. (Bitglass 2014) In addition to strong company policies, employee training should include coverage of:

- **Physical security -** Mobile devices, including laptops and smartphones, are often the target of thieves not only because they want to resell the device but also because they know the data on those devices can be far more valuable. Basics such as never leaving a computer or device in a car or unattended in public places still apply.
- **USB Flash Drives -** Transferring data with USB flash drives should be avoided. When absolutely necessary, use only company-issued encrypted USB flash drives and other external storage devices, and use security software to scan the devices. Physical protection of these highly portable devices is also crucial.
- **Restricting access to devices -** Allowing someone to access a computer increases the risk not only for malicious activity, but also unintentional damage such as the mistaken deletion of some files or execution of a prohibited or "blacklisted" program.

STEP 2. BUILD RESILIENCE AND PREVENTION

Organizations have recognized that resiliency is a key component of managing cyber risk. The detection and prevention of a cyber attack remains a critical and ever-present activity, however, ***resiliency – the ability to anticipate, prepare for, and recover from a cyber attack –*** should also be a point of focus. A resilient organization will have the ability to maintain its core purpose and operating integrity in the face of a cyber attack.

A recent study performed by IBM's Resilient and the Ponemon Institute found that 66% of organizations would be unable to recover from a cyber attack. Of the respondents, only 32% of IT and security professionals ranked their resilience as high. That same number was 35% in 2015, marking a drop over the past 12 months. One of the biggest hindrances to an effective recovery is a lack of a proper cyber security incident response plan. When it comes to cyber risk, many believe a cyber incident is a matter of "when" not "if." Planning for a wide variety of threats and outcomes will support faster recovery from cyber incidents.

To increase resilience when an unexpected event occurs, investing in Business Continuity Planning is smart business. There are myriad events that could impact a company's operations ranging from terrorism to weather to strikes to vendor outages. In the aftermath of 9/11, organizations have "upped their game" in this area which can be leveraged for cyber incidents.

All risk categories can result in a crisis situation that must be managed. However, compared to other risks, ***cyber risk can be instantaneous, impact a large number of users, be highly visible, and be difficult to remediate***. (As we saw in the recent reports on the Yahoo! breach, the identification of and related damage from the event can occur years later.) Social media and instant news feeds also accelerate the spread of the news, increasing the need for quicker response times. Consequently, it is imperative that appropriate planning be undertaken to ensure operations can continue and crises are effectively managed.

Planning and response frameworks fall into two highly related categories:

Business Continuity Planning

BCP represents the assessment of assets and exposures to develop an overall response plan throughout the organization. Generally performed at a business unit and/or activity level, this detailed assessment determines priorities during a disruption and plans to recover capabilities after a breach.

Incident Response

Incident Response covers how the organization will mobilize to deal with events impacting operations, including communication (internal and external), defining accountabilities for key activities, analysis and mitigation, and the resumption of normal operations.

A data breach does have some unique characteristics, but an incident response framework can be applied to any cyber incident with incremental adjustments for the nature of the event:

Baseline Stakeholders and Activities	Incremental for Cyber Risk
Key Team Members: • Impacted Business Units • In-house Counsel • Human Resources • Risk Management • Information Technology • Operations • Public Relations • Customer Relations • Investor Relations	**Specific Additional Experts:** ***Internal –*** • Privacy • Corporate Audit ***External –*** • Outside Counsel • Insurer and/or broker • Cyber Forensics • Crisis Communication Advisors
Baseline Activities: • Assess nature and impact of incident • Recover operations • Communicate with key stakeholders, including customers, regulators, senior leadership and board	***Additional Activities:*** • Taking impacted systems off-line • Resetting credentials, deactivating accounts • Notification to comply with privacy laws • Contacting law enforcement (typically FBI) • Cyber forensics

Establishing relationships with external experts and firms can support a more decisive response to a data breach. The post-breach environment is not the optimal time to be searching for required expertise or negotiating contractual terms, so having a team of external resources “at the ready” can speed recovery and resumption of operations. As noted earlier, insurance providers are able to support this activity as well.

Communication to senior leadership and the board is also critical in any disruption scenario. How companies respond to external stakeholders such as investors, customers, and regulators can make or break reputations in the period following a breach. (Through digital news feeds and social media, bad news travels very quickly.)

Practice and test. Don’t let the plans collect dust. Practicing and testing the protocols will help uncover any flaws in planning as well as get senior leadership comfortable with processes that are quite different than normal day-to-day operations. Similar to a fire drill, it is important to practice to detect process flaws and increase preparedness.

Step 3: Leverage Enterprise Risk Management to Enhance Cyber Security Management

The current landscape is summarized extremely well by Chris Halterman, CPA, Executive Director, Advisory Services for EY LLP and Chair of ASEC's Cybersecurity Working Group:

> *"The existence of multiple, disparate frameworks and programs for evaluating security programs and their effectiveness, as well as different stakeholders' preferences for each, has created a chaotic environment that only increases the burden on organizations trying to communicate how they design, implement, and maintain an effective cybersecurity risk management program."* (Tysiac, 2016)

The use of digital technology, and as a result, cyber security risk, is present in almost every business activity. Utilizing existing processes to assess and plan for cyber security risk will be more effective than implementing standalone parallel processes solely designed to cover cyber security risk. As noted previously, cyber security risk does need to be understood thoroughly and completely in its own right with customized tools, technology, and reporting, but capturing cyber risk in existing risk, governance, and decision-making frameworks will support those distinct assessments. Processes that should be reviewed for a cyber filter include:

Process / Activity	Cyber Filter Examples
Strategy	• What implications does our strategy for expanding or entering new products, geographies, or markets have on our cyber security risk profile? What new technologies will we need to implement in the next several years to serve our markets? What incremental cyber security risks are associated with these technologies? What steps need to be taken to be prepared?
M&A – Cyber Due Diligence and Planning	• What is the IT environment like at the acquired (or merged) company? What has their history been in terms of cyber challenges? How does the maturity of their (broadly speaking) cyber security practices compare to ours? What are the integration related challenges and costs?
Product Development	• What are the incremental cyber security risks associated with new products and how are those being mitigated, including any required IT investment? What are the implications to internal operating systems, customer access, third-party access, apps, employee training, etc?
Capital Allocation and Budgeting	• Are we spending sufficiently and effectively to combat cybercrime? Are the basics (patches, operating system upgrades, etc.) included in our financial plans? Where do we have gaps, and which are the most persistent? What is our peer group spending?
HR – Leadership and Succession Planning	• What are our projected human resource needs in cyber security? What are the recruiting, development, engagement, and retention mechanisms in place to ensure sufficient talent? What cyber experiences should our future leaders have?
Board and Management Agenda	• How frequently is the board and senior leadership looking distinctly at cyber risk? What summary reporting is available? What third party reporting or validation is available?

As discussed earlier, incorporating information security into ***vendor management programs, incident response frameworks,*** and ***talent planning*** is also an essential ingredient to more effectively manage cyber risk. Since companies have both standard and idiosyncratic processes, *all* processes should be reviewed to consider the benefits of any cyber decision-making criteria.

Closing the Cyber Security Risk Door

Incorporating a “cyber filter” into organizational processes will pay multiple dividends:

- ✓ Proactively capture cyber security related issues up-front to inform decision-making.
- ✓ Leverage protocols and mechanisms in place to increase efficiency and effectiveness.
- ✓ Provide clear, comprehensive, and consistent monitoring protocols for cyber related activities.
- ✓ Enhances cultural awareness by elevating and emphasizing discussions on cyber security risk.
- ✓ Facilitates a cross-functional, enterprise-wide approach to support a holistic, “birds-eye” view of a highly complex risk.

As organizations develop and evolve their cyber security risk management framework, they may uncover opportunities to upgrade other processes. For example, business continuity is a critical component of a recovery plan, but an organization’s existing baseline Business Continuity Program may be insufficient even before considering cyber risk. Other possible processes that may be in need of an update to fully accept the integration of cyber security risk include new product development as well as the management of third parties. As a result, savvy organizations will use the response and related investment in cyber security risk management to improve other aspects of their current governance, decision-making, and risk management practices.

CONCLUSION

In today’s operating environment, pursuing innovation, accelerating performance, and enabling growth are all highly dependent on successful technology-supported solutions. Technology is being incorporated into our personal and professional lives at an unprecedented and exponential rate. Consequently, cyber security risk is increasing at those same rates of change.

Creating value means taking risk. The classic risk and return paradigm applies to cyber security risk, notwithstanding its unique characteristics and pervasive nature. Cyber security risk can’t be avoided, but it can be managed. Developing a cost-effective strategy based on a consistent and comprehensive information security framework will go a long way to support a company’s security, resilience, and overall cyber security confidence.

About the Author

Mark Trembacki is a resourceful strategic cyber security and risk expert with substantial financial services subject matter expertise. He is the Founder of Risk Management Levers, Inc., a firm that confidentially assists companies with risk management (including cybersecurity, enterprise risk management, and reputation) and acquisition integration. Mark gained his experience in these areas during his career at BMO Financial Group (Bank of Montreal) where his latest roles were SVP, Risk Integration and COO, Commercial Banking, managing 200 employees and directing key enterprise risk management (ERM) initiatives across numerous business units and risk types — credit, market, operational, liquidity, business continuity, regulatory, fiduciary, and reputation.

In addition to an MBA in Finance from The University of Chicago Booth School of Business and a BS in Accounting with Highest Honors from the University of Illinois at Urbana-Champaign, Mark is a CPA who received the Elijah Watt Sells certificate for scores in the top 1% nationally. He is a SEC Financial Expert. He is currently earning his Cyber Security Management Graduate Certificate from the University of Virginia. In 2017, Mark expects to earn two certifications from National Association of Corporate Directors: the NACD’s Governance Fellow and the CERT Certificate in Cybersecurity Oversight. Mark is an active member of the American Institute of Certified Public Accountants (AICPA), focused on efforts to create accounting disclosure principles that more effectively describe cyber security issues. He is also currently an Adjunct Professor at the University of Illinois at Urbana-Champaign teaching Enterprise Risk Management in the Masters in Finance program and serves as Vice Chair of the DuPage Children’s Museum and is a Chicago Historical Society Board trustee. Mark can be reached via e-mail at trembacki@riskmanagementlevers.com.

References

Brecht, D. (2015, August 24). *Security Awareness and Spear Phishing - How to Stay Out of Danger*. Retrieved from EnterpriseAppsTech: http://www.appstechnews.com/news/2015/aug/24/security-awareness-and-spear-phishing-how-stay-out-danger/

Commission on Enhancing National Cybersecurity. (2016). *Report on Securing and Growing the Digital Economy.*

Forrester. (2016, October). *2017 Predictions:.* Retrieved from Forrester.com.

House Small Business Subcommittee on Health and Technology. (2013). *Small Business Cyber-Security Challenges With New Technologies.* Hearing Findings, Washington, D.C.

IBM. (2016). *2016 Cyber Security Intelligence Index.* IBM x-force Research.

Ipswitch. (2013). *Are Employees Putting Your Company's Data at Risk?*

Jaeger, J. (2016, November). Survey: Trials, tribulations of Third-party Risk Management. *Compliance Week*, pp. 1-3.

Martinez, O. (2014). Cybercrime to Cost you over $1M to Clean-up.

The Shared Assessment Program and Protiviti. (2016). *2016 Vendor Risk Management Benchmark Study.*

Tysiac, K. (2016). New Path Proposed for CPAs in Cyber Risk Management. *The Journal of Accountancy*.

Verizon. (2016). *2016 Data Breach Investigations Report.*

Wombat Security Technologies and the Aberdeen Group. (2015). *The Last Mile in IT Security: Changing User Behavior.*