The Compelling Case for Unifying IT and Physical Security

By Thomas L. Norman, CPP/PSP

The Compelling Case for Unifying IT and Physical Security

By Thomas L. Norman, CPP/PSP

Most organizations today follow the official plan. They have their building and critical rooms secured with electronic access control, digital video and security intercoms; their IT network secured with a firewall, anti-virus and anti-malware; their website secured and their email servers secured; and both physical security and IT security were installed by the best integrators they could find. Thinking they could now rest easy, knowing that they had taken all reasonable measures a prudent company should take … not knowing they were terribly vulnerable.

But security done this way is now just an illusion. The official plan is broken. The official plan has unknowingly become a plan for the organization's destruction. Yes, you read that right! That is not hyperbole. As you read this, organizations *are* being destroyed right out of business by the new landscape of security threats. And these are threats that *cannot* be secured using traditional strategies.

The target landscape for threat actors today is rich and safe for the threat actors. More sophisticated modern attackers are uncovering and utilizing cross-platform exploits that use the cracks *between* physical and IT security systems to attack the organization. This approach is new, like ransomware was new just a couple of years ago. But today, more than half of malware attacks carry a ransomware payload. In a couple of years, it is likely that cross-platform attacks will be very common, and existentially destructive.

This paper outlines how there is no longer any security without a holistic hi-tech, lo-tech, no-tech approach to security, including both IT security and physical security as a single approach, and how organizations can address the new combined threat landscape in a new, much more effective way.

When applying security measures, organizations are interested in applying countermeasures to those threat scenarios that are:

- most likely to occur
- most serious in terms of damage to the organization[1]

This paper focuses on threat scenarios that are most likely to occur and which have the very real potential to seriously damage or destroy the organization's financial viability. This is particularly true for small and medium business enterprises.[2] And while the threat scenarios

1. Items 1 and 2 above are both referenced from Rand Corporation, "Emerging Threats and Security Planning – How Should We Decide What Hypothetical Threats to Worry About," Rand Occasional Paper, Homeland Security Division, 2009, Rand Corporation.

2. PCI Fines for SMB businesses can reach up to $100,000 per month of non-compliance, possibly bankrupting some SMB businesses. PCI NonCompliant Consequences, <http://www.focusonpci.com/site/index.php/PCI-101/pci-noncompliant-consequences/Print.html>

discussed herein probably do not have the potential to destroy an enterprise organization, it is most certain that the shareholders and the public press would take notice of the incident and its aftermath. Such incidents would almost certainly damage the organization's business reputation, which would compound the financial damages of the actual incident, and the direct costs to mitigate the incident.[3]

Security threat scenarios, particularly IT security threat scenarios, have transformed in the last few years from incidents that we *should* pay attention to, into incidents that are real existential threats to the organizations they are striking.[4] Many organizations are simply closing their doors in response to these threats, and that is not an exaggeration. These are incidents that simply must be prepared for, for the welfare of the organization, its management, its employees and the community that it serves.

These incidents are very real. They are happening to organizations every day. You are reading about them in the news, with a sigh of relief saying "I'm sure glad that didn't happen to us!" But the odds are seriously stacked against you. These incidents *will* strike most organizations within the next few years.[5] This paper discusses what they are and how organizations can *effectively* mitigate the likely damages that will occur.

Let's take a look at a few examples of why this is so important.

IT Security is at Risk of Physical Attack Now More Than Ever Before

Case 1: The National Security Agency (NSA)

The NSA is responsible for acquiring intelligence worldwide from communications sources, primarily technology sources. This includes phones, radios and information technology networks, including the internet, dark web (an "off the internet" shadow internet where many illegal things are offered for sale, including malware kits and information on how to break into networks), TOR and private networks. The scope and depth of NSA capabilities at gathering data is simply astonishing. To perform this role, the NSA has developed highly proprietary methods for breaking into networks all over the world, carried out by a specialized hacking team of unparalleled sophistication, reportedly known simply as the Equation Group, making them quite probably the largest and most prolific hacker organization in the world, their scope being approached only by other similar agencies from Russia, China, Iran and Great Britain. Intrinsic in their mission is a focus on protecting their technology, methods and tradecraft, and the results of their exploits.

3. *CSO Magazine*, "Does a data breach really affect your firm's reputation?" by Doug Drinkwater, CSO, January 7, 2016.

4. *Chief Executive Magazine*, "Existential Threats: 5 Tips for Educating Boards on Data Security" by Brian Stafford, February 17, 2016, <http://chiefexecutive.net/existential-threats-5-tips-for-educating-boards-on-data-security/>

5. *Security InfoWatch*, "When will your data breach happen: Not a question of if but when," by David Barton, March 10, 2015.

In August 2016, news came that the NSA itself had been hacked[6], possibly by Russia.[7] The recent security attack on the National Security Agency was both audacious and very effective. The news came in the form of exploit kits being sold on the dark web. Offered for sale there were a number of exploit kits used exclusively by the NSA to break into common firewalls and routers by virtually every major manufacturer. In other words, what many would consider the crown jewels of the NSA!

Sources within the NSA who don't want to be quoted say that this incredible "hack" was not a hack at all. It was instead the result of an insider with critical access who simply walked out the door with a USB chip full of the NSA's top secrets.[8] In other words, it was a physical security exploit, not an IT security attack.

The federal security agency most capable of IT security lost its crown jewels to a physical security exploit!

More on the NSA "Hack"

As this paper is being written, the forensics on the NSA attack are underway. Early indications are that this was a Russian FSB operation, aimed at embarrassing the Obama administration. The material posted on the Dark Net included scripts from 2013 such as one called "Extra Bacon" that could gain access to common firewalls (in this case, the Cisco ASA firewall). However, the Cisco ASA firewall has had a major upgrade since this script was written that would make it impossible to use against newer versions, only working on older versions that have not been updated. So far, all exposed scripts are from this era. This indicates that the insider was not directly part of the famed "Equation Group," but someone else who worked peripherally around that group, who had only limited access to current scripts.

Case 2: Veteran's Administration (VA) Massive Data Breach

Personal identifying information on about 26.5 million U.S. military veterans was stolen from the residence of a Department of Veterans Affairs data analyst who took the material home in violation of VA security policies.[9] The data stolen included names, Social Security numbers and dates of birth of the veterans. Inside sources have reportedly claimed that the data are from the VA Benefits Administration branch. If so, such data would also likely contain ratings and entitlements as well. Such information would typically also contain the amounts of VA disability deposits and the account numbers and routing numbers of banks into which such deposits are to be made. 26.5 million information technology records of the most vulnerable among us, lost to a physical security breach.

6. Cato Institute, "CATO at Liberty," by Julian Sanchez, August 19, 2016, <http://www.cato.org/blog/nsa-hackers-hacked?gclid=CKGF15aK2M4CFdg9gQod_P8Ftw>

7. *Business Insider*, "Edward Snowden: Russia might have leaked alleged NSA cyberweapons as a warning," by Rob Price, August 16, 2016, <http://www.businessinsider.com/edward-snowden-shadow-brokers-russia-leaked-nsa-equation-group-files-warning-dnc-hacking-2016-8>

8. *ARS Technica*, August 22, 2016, "Hints suggest an insider helped the NSA "Equation Group" hacking tools leak," by Sean Gallagher.

9. *SC Magazine*, "U.S. Veteran Affairs Department settles data breach case," by Chuck Miller, January 28, 2009, <http://www.scmagazine.com/us-veteran-affairs-department-settles-data-breach-case/article/126518/>

Case 3: DDOS Attack Using 25,513 IP Video Cameras from 105 countries

Just when you thought it was safe to go back into the water, researchers from the security firm Sucuri discovered that in a very unique attack, 25,513 internet-connected IP security video cameras (physical security devices) have been connected into a massive denial-of-service botnet used in a "proof of concept" distributed denial of service (DDOS) attack against a jewelry store site.[10] The source article indicated that this massive botnet was generating nearly 50,000 HTTP requests per second. However, Jason Thacker of White Badger Group, LLC, a leading cybersecurity consulting group, states that it is more likely that these were not HTTP requests, which would require running malware on the cameras, but rather simply HTTP/RTSP streams, which could run from unmodified cameras. The attack continued for days and researchers found that the botnet had leveraged only Internet of Things (IoT) CCTV devices from 105 countries.

This attack is truly unique. It is believed that absolutely nothing can stand up against an attack of this magnitude. Not Google, not Amazon, not the U.S. military, not anything. Further, this attack was primarily launched from IoT security CCTV devices that had been reprogrammed into multicast mode. While many believe that they should be safe against a multicast DDOS attack because they have not subscribed to it, in fact, the multicast server holds the subscription list. And that list can include any group of IP addresses, or range of IP addresses. The range could include a jewelry store, all the IP addresses served by an individual ISP, or something as large as the IP address range including the entire United States of America (however an attack of this scale is highly unlikely due to the demands on the multicast server). And all executed within milliseconds with no obvious weaponry. Obvious defenses against an attack like this include sending out multicast unsubscribe messages to the multicast servers. This would be effective because it would have an asymmetric effect against the attackers, in favor of the defenders. Thanks to Jason Thacker, CISSP, CEH, vice president and chief technology architect, White Badger Group for information on multicast attack and defense strategies.

Is Physical Security at Risk of Hacking?

Case 4

A worker at a Ukraine electrical distribution plant control center was ending his shift when he was stunned to see the cursor suddenly move across the screen and click on buttons that opened the circuit breakers that took the substation offline.[11] The worker stared in disbelief as he watched the cursor move to a dialog box on the screen to confirm that the circuit breakers were to be taken offline.

In that moment, thousands of residents had just lost their lights and heaters.

10. *ThreatPost*, "Botnet Powered by 25,000 CCTV Devices Uncovered," by Chris Brook, June 28, 2016 <https://threatpost.com/botnet-powered-by-25000-cctv-devices-uncovered/118948/>

11. *Wired Magazine*, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," by Kim Zetter, March 3, 2016 <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

The operator found that the mouse would not respond to his commands and continued to take additional breakers offline. Then, the machine logged him out of the control panel. Trying to log back in, the worker found that his password had been changed, and he could not regain control of the system. All he could do was stare hopelessly at the screen as the machine clicked off breaker after breaker, taking 30 substations offline. At the same time, two other power distribution centers were hacked, plunging 230,000 residents into the dark and the cold of winter. The operators themselves were fumbling in the dark. Real physical damage from a cyberattack.

Case 5

In 2008, cyber terrorists hacked into the majority BP-owned Baku-Tblisi-Ceyhan pipeline in Turkey causing an explosion with flames as high as 150 feet.[12] Previously, the Baku-Tblisi-Ceyhan was believed to be one of the most secure pipelines in the world. But in this attack, the terrorists infiltrated the pipeline through a wireless network, tampered with the systems and caused severe physical damage. The U.S. has millions of miles of pipelines that distribute oil, hazardous liquids, natural gas and chemicals. Many of these can be reached above ground simply by walking up to them (providing for physical attacks) and also seem to be vulnerable to cyberattacks that can inflict the same kind of serious physical damage as physical attacks.

NSA Director Admiral Michael Rogers said in November 2014 that several foreign governments had already hacked into U.S. energy, water and fuel distribution systems, potentially damaging essential services, according to Bloomberg.

Case 6

At a recent DEFCON conference, Dennis Maldonado, security consultant at KLC Consulting showed exactly how to hack into a variety of common access control systems, providing access to anywhere in the facility to persons who had no authorization whatsoever to be there.[13] Physical access via a cyberattack.

At another DEFCON, Jason Ostrom and Arjun Sambamoorthy demonstrated how to hijack various common video surveillance systems and extract, record and replace video on their servers, providing attackers a way to replace video of a physical intrusion with looped video showing no intrusion.[14]

12. *Bloomberg Technology News*, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," by Jordan Robertson and Michael Riley, December 10, 2014, <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>

13. DEFCON Communications Inc., DEF CON 23 Presentation by Dennis Malsonado, KLC Consulting, <https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Dennis-Maldonado-Are-we-really-safe-bypassing-access-control-systems-UPDATED.pdf>

14. ViperLab, Sipera Systems, DEF CON 17, "Advancing Video Attacks with Video Interception, Recording, and Replay," by Jason Ostrom and Arjun Sambamoorthy, July 31, 2009, <https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-ostrom-sambamoorthy-video_application_attacks.pdf>

Case 7

As a global security consultant, I sometimes get called to evaluate system weaknesses. Here's an example of one involving a physical security vulnerability to IT attacks.

At an overseas facility that had switched out all of its exterior analog security video cameras for IP cameras, I noticed that bare IT cables were attached to a wall in a publicly accessible parking structure (one could simply walk into the structure). Following the cables, I discovered that the cable was an un-conduited connection to a small consumer-grade digital switch contained within an electrical panel near the parking gate.

This panel sat on a raised curb next to an adjacent parking space, and the door swung into a walkway next to the parking space, making the panel accessible to the parking space. The lock on the panel was broken, so it could be opened by anyone and there was no tamper switch on the panel, so no alarm would have been reported upon opening the panel. The digital switch inside the panel served several IP cameras, two security intercoms and an access control panel, all located near the parking gate.

Sniffing the connection, we realized that unencrypted traffic on all of these systems flowed through the digital switch. This parking space provided unhindered access to the security system IP network including the video servers and access control system servers. In other words, using information readily available on the internet, this security system could be hacked into while sitting in a car in the public parking structure, providing the hacker with the ability to remotely unlock vehicle gates and doors, bypass alarms, guide the intruder through the facility and into the most restricted areas of the facility, and after having left, he could overwrite the video with looped video showing no intrusion during the time period of the intrusion. Because this was an enterprise-class system connecting every facility in the organization, the hacker could gain entry to any facility in the entire enterprise, all from the comfort of his car.

This would classify as a failure of both IT and physical security for the organization on a colossal scale. And we see things in some way like this almost every month.

IT and Physical Security – Or Just One Security Model Including Both?

Have one goal: overlapping security. Understanding that IT security attacks often involve physical security breaches and physical security breaches sometimes involve IT security hacks means a dedication to both is necessary.

From the illustrations above, we can see that an organization's physical security and their IT security are each at risk from vulnerabilities in the other. One cannot secure their organization without securing both properly. Each is dependent on the other. While lawsuits against organizations involving physical security insufficiencies abound, failure to comply with IT security requirements, particularly HIPAA (Health Insurance Portability and Accountability Act) compliance, can have truly profound and devastating effects on the organization and individuals within the organization who violate HIPAA guidelines and regulations. In one case in 2010, a former UCLA Healthcare System surgeon was sentenced to four months in prison for a HIPAA

violation.[15] In April 2013, Helene Michel, the former owner of a Long Island, N.Y., medical supply company, was sentenced to 12 years in prison in a case that included criminal HIPAA violations.[16]

Compliance violation fines can also be severe. In 2014, a New York Hospital and major university were fined $4.8 Million for HIPAA violations.[17] Small businesses are not immune either. Mom and pop businesses have been hit with fines and remediation costs, legal fees and others totaling up to six figures.[18] Since October 2006, Visa has levied $3.3 million in fines for post-incident discovery of non-compliance, with more than 80 percent of the credit card breaches having occurred at small businesses.[19] It's not any better for enterprise class organizations. "… Target incurred a $162 million loss over 2013–2014 after its data breach, in addition to experiencing a staggering 46 percent drop in profits in the Q4 2013 holiday shopping season immediately following the attack. More recently, the company has agreed to pay $67 million to financial institutions that issued credit cards for which the security was compromised in the breach. And now the courts have opened the gates for banks affected by the attack to file additional class action suits against the retailer."[20] And this does not include the long-term loss of business due to the damage to their business reputation. Data loss incidents can be very, very expensive.

The "Ponemon Institute 2016 Cost of Data Breach Study: Global Analysis" reported that the average organizational cost of data breach in the U.S. rose from $5.85 million in 2014, to $6.53 million in 2015, to $7.01 million in 2016.

So compliance with IT security standards is essential to the welfare of the organization, whether large or small. It is essential then, that organizations large and small secure both their IT systems and data, and their physical access to the facility containing sensitive information, whether in paper or binary form.

15. *Outpatient Surgery*, "UCLA Researcher Gets Jail Time for HIPAA Violations," April 2010, <http://www.outpatientsurgery.net/surgical-facility-administration/legal-and-regulatory/ucla-researcher-gets-jail-time-for-hipaa-violations-corrected-version--04-29-10>

16. *InfoRiskToday*, "Prison Term in HIPAA Violation Case," by Marianne Kobasuk McGee, February 20, 2015, <http://www.inforisktoday.com/prison-term-in-hipaa-violation-case-a-7938>

17. HHS.gov, "Data Breach Results in $4.8 Million HIPAA Settlements," May 7, 2014, <http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html>

18. *PMQ Pizza Magazine*, "Don't Let Credit Card Fraud Put You Out of Business," by Tracy Morin, May 2016 <http://www.pmq.com/May-2016/Dont-let-credit-card-fraud-put-you-out-of-business/>

19. Braintree, "PCI Compliance Fines for Small Business Breaches," October 17, 2007 <https://www.braintreepayments.com/blog/pci-related-fines-for-breaches-at-small-businesses/>

20. *Chief Executive Magazine*, "Existential Threats: 5 Tips for educating Boards on Data Security," by Brian Stafford, February 17, 2026, <http://chiefexecutive.net/existential-threats-5-tips-for-educating-boards-on-data-security/>

A Compliance-Based Data Loss Protection Plan

A comprehensive IT/physical security program requires a plan. Nearly every organization today falls under one or more data privacy compliance standards.[21] This is not only one of the best ways to start a data protection plan, but to take any other approach risks putting the organization into non-compliance and subjecting it to legal penalties.

The major compliance standards include:

- **HIPAA (Health Insurance Portability and Accountability Act):** HIPAA applies to any business that touches health care records with personally identifying information (PII), including hospitals, clinics, senior care facilities, pharmacies, even janitorial firms and security firms, etc., that could see such records in a health care environment.
- **SOX (Sarbanes Oxley Act of 2002):** SOX is designed to protect shareholders and the public from accounting errors and fraudulent practices from affected organizations.
- **FISMA (Federal Information Security Management Act of 2002):** FISMA protects government information, operations and assets against natural or man-made threats.
- **GLBA (Gramm Leach Bliley Act):** GLBA requires many companies to protect themselves against unauthorized access, anticipate security risks, and safeguard a consumer's nonpublic information. It also prohibits individuals and companies from obtaining consumer information using false representations. GLBA also gives consumers privacy notices that explain the institutions' information-sharing practices.
- **FERPA (Family Educational Rights and Privacy Act):** FERPA gives parents access to their child's education records, an opportunity to have the records amended, and some control over the disclosure of information from the records.
- **PCI/DSS (Payment Card Industry Data Security Standard):** PCI/DSS is the premier compliance standard in the private sector and it applies to any business or individual that is processing payments by Visa, MasterCard, American Express, Discover and JCB. Companies and organizations perform validation annually, by an external qualified security assessor (QSA) or by a firm-specific internal security assessor (ISA) who creates a report on compliance (ROC) for those companies that are processing large volumes of transactions. For smaller companies, a self-assessment questionnaire (SAQ) is used.

These are the most common data privacy protection compliance standards. There are additional federal, state and contractual standards that may apply.

There is a huge security exposure for any organization accepting credit card payments. These businesses are easy targets for hackers due to the inadequate technical security provisions available from the credit card industry, and the penalties and all of the risk have been pushed down from the financial institutions and payment processors, down to the companies that accept credit cards. Finally, the financial penalties for non-compliance for businesses that accept credit cards can be crushing, especially on small and medium-sized businesses.

21. *Business Law Today,* "The Practical Tech Lawyer: Advising a Company on Data Security Compliance," by Theodore F. Claypoole, November 2014, <http://www.americanbar.org/publications/blt/2014/11/04_claypoole.html>

It is unlikely that any single organization will be held accountable under more than a few of these requirements. But it is certainly necessary for every organization today to understand which standards and acts they are held accountable under. Remember, penalties for non-compliance can be severe, and for small businesses, it could mean the end of their business.[22]

The following is a 10-point plan to get any organization to full compliance with government (HIPAA, SOX, FERPA, GLBA and FISMA, etc.) and contractual obligations (PCI/DSS), and can also help secure the treasured data from unauthorized access, disclosure and harm.

1. Get a "C-Level" Commitment to Security

C-level executives set the culture for the entire organization. Others follow their example. When a C-level executive short-cuts security measures, you can expect that others will too. When they are scrupulous in following security policy, others will be too. So commitment from the "C-suite" to security policy is essential to the success of the program, and essential to the success of the organization. This commitment minimizes not only the organization's risk of security incidents themselves, but also minimizes the organization's risk of findings of negligence related to a compliance-involved security breach, which may occur no matter what security measures are taken. It is important to understand that security breaches do occur, even to the best prepared organizations (the NSA, for example). And when the compliance auditors come to examine the breach, a finding that the organization has taken reasonable measures to prevent and mitigate a breach goes a long way towards keeping any compliance fines as low as possible, or nothing. Obvious non-compliance, the lack of a coordinated security program either in IT security or physical security can result in six-figure fines, and for some individuals, jail time.

One of the C-level executives should be named as the chief security compliance officer. This is essential because, in the event of a compliance-related security breach, the C-suite *will be held responsible* by the compliance agency for the breach and may in some cases be held individually responsible for fines and other penalties. It is far better for a C-level executive to take that responsibility on so that the security program has guidance from a company officer who is committed to the success of the program, and the authority to ensure that commitment is followed by everyone in the organization.

2. Know Your Legal Obligations for Data Protection

Few organizations thoughtfully realize that security is part of the core mission of their organization.[23]

Every organization begins with a mission. It develops programs in support of that mission, and those programs acquire four kinds of assets:

- people: employees, contractors, vendors and customers

22. *Thomson Reuters*, "Demonstrating how non-compliance can mean the end of a firm or career," December 3, 2014, <http://thomsonreuters.com/en/articles/2014/demonstrating-how-non-compliance-mean-the-end-of-a-firm-or-career.html>

23. *InformationWeek*, DarkReading, "It's Time to Treat Your Cyber Strategy Like a Business," by Jason Polancich, January 9, 2015, <http://www.darkreading.com/messages.asp?piddl_msgthreadid=22391&piddl_msgid=278778>

- property: real property, fixtures, furnishings and equipment including IT systems
- proprietary information: information to be safeguarded, especially under mandated compliance requirements
- the organization's brand: the business reputation of the organization

Intrinsic in the sustainability of any organization is the obligation to keep those four classes of assets secure. Organizations often think of security as a non-revenue producing business unit that usually cannot display its value as well as, for example, the accounting department can. But a relaxed attitude about security can lead to disastrous results, especially in compliance areas.

Every organization must know the compliance standards that it is mandated to follow. Ignorance of such is not an acceptable excuse.

- Compliance standards may emanate from federal or state laws or regulations, and are enforced by federal or state agencies, or by civil or criminal lawsuit.
- Compliance standards may also emanate from private contracts with other organizations, such as financial or health care institutions.

Many small and medium-sized businesses may not even be aware that they are legally obligated to follow specific compliance standards, those legal obligations being part of a private contract that the organization may have signed. Those obligations have legal and financial ramifications.

The two most common ways to determine what compliance standards your organization is required to follow are to find an attorney who specializes in data loss protection compliance law, or to use a software program such as ZenGRC from Reciprocity that walks you through a series of questions to determine which federal, state and commercial compliance standards may apply to your organization.

Understand What Assets Need Protection

Classify your assets by criticality. The top critical assets of every organization include:

- people
- business operations
- business reputation (the brand)
- proprietary information, especially compliance-related information that the organization is legally obligated to protect and defend

3. Define Your Risks

The simplified risk formula R = P*V (Risk = Probability * Vulnerability) includes the probability of threat scenarios occurring multiplied by vulnerability.

IT security vulnerabilities include, among others, poor user authentication, inadequate and misconfigured firewalls, failure to read logs, rogue access devices, company data stored on personal devices, mobile devices, and unpatched and unpatchable devices.

IT security threats include disgruntled and negligent employees (insider threats), third-party service providers, malware (especially ransomware), targeted hacking and email phishing, among others.[24]

Key mistakes include overreliance on security monitoring software, technology innovations that outpace security provisions, outdated operating systems, lack of encryption, organization data on unregistered user-owned mobile devices, IT "diplomatic immunity" within your organization, lack of management support, challenges recruiting and retaining qualified IT staff, and failure to segregate IT security audit duties.[25]

Firms should understand the source of threats and weigh the probability of being struck by each. For example, malware and phishing attacks have a much higher likelihood of occurring than a targeted attack. However the potential for damage from a targeted attack, if carried out, is much higher; especially against highly proprietary information such as compliance mandated PII, trade secrets, patents, formulas and the business reputation, etc.

Then, perform an IT system audit to evaluate the system vulnerabilities. This includes:

- data loss protection measures (for data at rest and data in motion)
- data backup measures (frequency, completeness and immunity from ransomware) … and don't forget backup images of servers and workstations (operating systems, applications and configurations)
- map the infrastructure
- map the endpoints including wired, wireless and mobile devices including printers
- map the operating systems in use by all servers and endpoints, ideally including patch/update status
- review the IT security policies and procedures
- review applications in use and their update status (understand that some applications may not be compatible with the latest patches of certain software on the machine, for example some apps may not work with the latest version of Flash, or the operating system may not be compatible with the latest version of an application … hint: operating system update is indicated)

All of this above establishes the IT security risk (R=P*V).

4. Perform a Gap Analysis

Compare what the organization is legally required to do for IT security (from a mandated compliance standpoint) with the vulnerabilities exposed in the system audit. The delta is the gap that must be filled to be compliant. This forms the basis for the IT security implementation plan, which typically includes factors such as:

24. Includes information from: *CIO Magazine*, "6 Biggest Business Security Risks and How You Can Fight Back," by Jennifer Lonoff Schiff, January 20, 2015, <http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html>

25. Includes information from: Berry Dunn, "The Top 10 Information Security Risks for 2015," <http://www.berrydunn.com/news-detail/top-10-information-security-risks>

- existing equipment and software (determines compatibilities and incompatibilities)
- business culture (determines user interfaces, if applicable)
- financial issues (for example, can the organization afford managed services vs. something less proactive?)
- end user preferences, if any

5. Set Forth an IT Security Implementation Plan

The gap analysis will help create a roadmap for what policies, procedures, hardware, software and configurations are needed to bring the IT system from where it is now relative to full compliance, to where it needs to be to achieve full compliance.

- Create an implementation plan from the gap analysis.
- Budget and acquire necessary hardware, software and third-party assistance to implement the plan, prioritized by the highest priority assets and any exigent emergencies.
- Schedule the implementation plan based on priorities above.
- Implement controls for the minimum acceptable downtime.
- Verify system operations after *each* part of the implementation plan to be sure that one doesn't need to step back due to an incompatibility.
- Verify that the desired readiness to pass a compliance audit is reached.

6. Define the Physical Security Risks

The same four top critical assets apply to physical security for the organizations:

- people
- business operations
- business reputation (the brand)
- proprietary information, especially information that they are legally obligated to protect the privacy of

Again, Risk = Probabilities * Vulnerabilities. Probability is comprised of the applicable threat scenarios.

Determine Possible Threat Actors and Likely Threat Scenarios

Physical security threat actors may include terrorists, violent criminals, economic criminals, activists and petty criminals.

The possible threat scenarios will depend on the physical environment at the facility and the existing countermeasures in place. It is best to retain a qualified consultant to determine possible threat scenarios. Malicious IT threat actors who would gain access through physical vulnerabilities should be included in the threat scenario mix. From the list of considered scenarios, estimate the probabilities prioritized by asset criticality (focus on people).

Assess the Physical Security Vulnerabilities

An assessment of the organization's physical security vulnerabilities should include a review of:

- where unauthorized access may be occurring, or could occur
- where entrances and exits to critical spaces may not have a quality working security video camera
- where undetected and/or unobserved intrusions could occur to the property, the buildings and critical areas within the buildings
- the access control process to make certain that access credentials are sufficient, up-to-date, and that the access control database is current and that granted access areas are kept up-to-date to be appropriate for the users
- the physical security policies and procedures, including hiring background checking as it relates to security vetting, and look for any discrepancies against the needs of the organization
- current security staffing to be certain that it fits the current needs of the organization

Calculate the Risk: Risk = Probability * Vulnerability

7. Perform a Physical Security Gap Analysis

Review the risk analysis and create a gap analysis from the remaining vulnerabilities after looking at the risk minus the existing mitigating measures.

8. Create a Physical Security Plan

From the gap analysis, create a proposed physical security implementation plan, which will include:

- update to physical security policies and procedures
- policy driven vulnerability patches (additional card readers, alarm points, video cameras, intercoms, etc.)
- updates to security staffing, if needed
- budget and acquire necessary security hardware, software, configurations and staffing
- implement the plan
- review the results to be sure it is meeting the needs of the organization

9. Training and Testing

Both IT security and physical security policies need to be pushed out to employees in a way that can help ensure the success of the program. Employees who are not aware of security policies cannot be expected to follow them. Review C-suite security policy compliance and remind if necessary that employees emulate what they see from upper management.

Employee training and compliance involves five elements:

- Update the employee policy manual and ensure that all employees sign off on the updates.

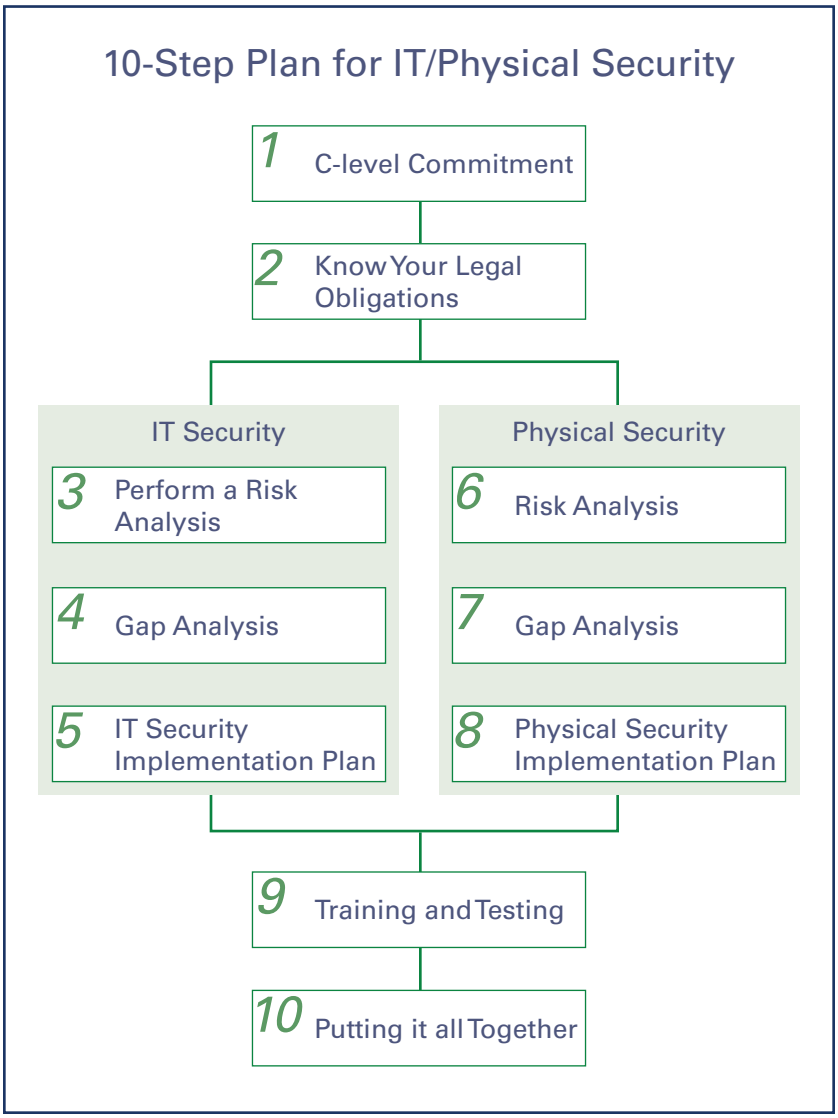
- Provide ongoing training on areas of widespread non-compliance.
- Counsel individual employees on individual non-compliance.
- Test employees on compliance (bait phishing emails, be observant of employees who indicate resistance to security policies and may have expressed a willingness to circumvent the security policies and record the non-compliance for counseling).
- Discipline (advisory notice, up to termination) for repeated evidence of non-compliance.

10. Putting it all Together

When developing the security plans for both IT security and physical security, pay special attention to how cyber risks can create physical security vulnerabilities and how physical security risks can create cyber vulnerabilities.

Cyber risks that can create physical security vulnerabilities:

- IP devices outside the skin of the building that are not on their own VLAN and firewalled
- digital switches that have open unused ports
- no VLAN between the physical security system and the organization's business network
- shared physical security/business IT system servers
- unencrypted communications on the physical security system (should be encrypted all the way to the endpoints)
- switches that are not "locked" onto the MAC address and (if possible) the chipset of the attached endpoint, allowing a replaced device attack



- switches that are not configured to lock out any device if the connected device is disconnected (I know, it's a pain to reprogram each time you replace a failed device, but this configuration completely blocks anyone who unplugs a device and tries to tap into the new open port.)

Physical security vulnerabilities that can create cyber risks:

- Pay attention to employee vetting. Ask the NSA about Edward Snowden, ask the Army about Private Bradley Manning, ask any organization about the one they took just because he looked good to the interviewer and turned out to be a criminal afterwards. Every organization needs to have good criminal background and psychological vetting. And trust me, criminal background vetting can be done in a way that does not violate a paroled or fully served criminal from getting a good job. Just don't allow a person with a criminal history in say, identity theft to get anywhere near personal identifying information.
- Keep all cabinets with IP connection in them locked and fitted with an operating tamper switch.
- Ensure that all digital switches, routers and servers are located behind locked doors (that are kept locked!), and the rooms they are in are fitted with motion detectors and security video cameras.
- Keep security servers in locked racks fitted with tamper switches.
- Keep video cameras viewing sensitive areas out of the view of the public or non-qualified viewers.
- Make sure that the physical security system is firewalled and equipped with an IP intrusion detection system and that the firewall and server logs are viewed or audited daily (best if by automated software, followed by a qualified analyst or manager for the filtered log report).
- Disconnect all USB and DVD drives on security workstations except for the workstation that is designated to export security text reports and video incident report DVDs.

Summary

Both IT security and physical security will always have exposed vulnerabilities. Increasingly skilled threat actors look for and exploit these vulnerabilities within each discipline, and increasingly across the chasm between IT security and physical security. There really isn't a line anymore. Vulnerabilities in one system can and are easily being used to exploit the other. Compliance driven requirements can present great exposure to the organization, where vulnerabilities can be exploited. Organizations should blend both physical security and IT security programs for their own welfare, using specialists in each domain who work together to seal the doors against determined threat actors. This additional element will also further assist in reducing the organization's liability exposure for any compliance breaches that may occur.

The risk model outlined in the paper is a simplified risk model (to keep the text within length). Each of the elements discussed herein contain other constituent components that may need to be explored, especially if the case in point is an enterprise-class organization.

Constituent Components

Risk components:

- probability (or likelihood)
- vulnerability
- (rank risks by consequences)
- consequences (can be applied to each asset)
    - asset value to the sustainability of the organization
    - asset value to ongoing operations
    - asset value in terms of direct and indirect costs of a breach

Probability components:

- threat scenarios
- likelihood

Vulnerability components:

- accessibility
- surveillance opportunities
- intrinsic vulnerability (with no countermeasures)
- natural countermeasures
- physical measures (locks, barriers, fences, lighting, etc.)
- electronic measures (access control, video, communication, etc.)
- operational measures

Thomas L. Norman (tnorman.ppi@gmail.com) is global security consultant for Ingram Micro (http://www.ingrammicro.com/).

