CHAPTER

# 1

# RISK MANAGEMENT DIGITAL STYLE

*Which risks are relevant? Those that impact business goals.*
*Which risks impact business goals? They all do.*

Did you hear the one about the IT security officer who "resigned" after it was discovered that a data breach at its retail operations headquarters that affected millions of customers could have been avoided if only one of over 60,000 alerts had been heeded?[1] Or the one about a security consultant who leaked information about a government surveillance program, bringing world leaders to the defense, who ended up exiled in Russia but had a great turnout at South by Southwest?[2] Or how about the one of

[1] Target Data Breach, 2013.
[2] Edward Snowden, NSA leak, 2013.

**Managing Online Risk**

computer engineers who lost their life savings and their jobs in the misplacement of digital currency?[3] Or the one about the employee who left a company laptop connected to public Wi-Fi at the coffee shop that led to insider trading violations and criminal penalties?[4] Or the one…

I think you get the point. There have been a lot of "ones" in the news and even more not in the spotlight. In 2011, Verizon reported "855 incidents and 174 million compromised records."[5] To update that, the Online Trust Alliance (OTA) released their report in January 2014, which indicated that of over 500 data breaches in the first half of 2013 "31 percent of incidents were due to insider threats or mistakes; 21 percent resulted from the loss of computers, hard drives, and paper documents; 76 percent were due to weak or stolen account logins and passwords; and 29 percent of compromises resulted from social engineering."[6] What do these have in common? They all dealt with information technology in the online digital environment.

As we begin our exploration of online risk and security, it is useful to make sure we are on the same page. Defining the lexicon of the landscape allows us to define risk management and security in the context of the digital environment and determine whether they are different because of this new context or because they have they just been expanded. Therefore, we begin with standard definitions of risk management, risk, security, and threat. You may have your own favorite you use, but we will stick with these as we head out.

*Risk management*

The identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks.[7]

*Risk*

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.[8]

*Security*

The prevention of and protection against assault, damage, fire, fraud, invasion of privacy, theft, unlawful entry, and other such occurrences caused by deliberate action; the extent to which a computer system is protected from data corruption, destruction, interception, loss, or unauthorized access.[9]

[3] Mt. Gox and their misplacement of Bitcoin, 2014.

[4] Raj Rajaratnam of the Galleon Group, 2014.

[5] Verizon, 2012 Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[6] Pangburn, DJ, "2013 Was the Worst Year for Data Breaches," Motherboard Blog, http://motherboard.vice.com/blog/2013-was-the-worst-year-for-data-breaches, January 23, 2014.

[7] "What is Risk Management? Definition and Meaning," http://www.businessdictionary.com/definition/risk-management.html#ixzz2ZsV0ylRk (accessed 2/8/2014).

[8] "What is Risk? Definition and Meaning," http://www.businessdictionary.com/definition/risk.html#ixzz2ZsV8eFjd (accessed 2/8/2014).

[9] "What is Security? Definition and Meaning," http://www.businessdictionary.com/definition/security.html#ixzz2ZsVYEske (accessed 2/8/2014).

*Threat*

Indication of an approaching or imminent menace; negative event that can cause a risk to become a loss, expressed as an aggregate of risk, consequences of risk, and the likelihood of the occurrence of the event. A threat may be a natural phenomenon such as an earthquake, flood, or storm, or a man-made incident such as fire, power failure, sabotage, etc.; action or potential occurrence (whether or not malicious) to breach the security of the system by exploiting its known or unknown vulnerabilities.[10]

Most of those definitions should seem familiar to you. However, there are some key words within them that bear special consideration as we look at online security and risk management. First, risk management brings up the issue that there are acceptable and unacceptable risks—what would be an acceptable risk has long been debated by security professionals. One school of thought is that any risk is unacceptable. The other believes it is a return-on-investment (ROI) question—how much does it cost to mitigate the risk versus how much will the risk impact cost if left alone?

Second, notice that the definitions of risk and threat are symbiotic with two main differences: a threat is indicated as something that can be foreseen and is imminent; a risk is just a probability. But both indicate that they can be avoided to a certain extent—excluding natural disasters.

Third, security is presented to offer a safety net around property—whether tangible or intangible, such as online data. And last, risk management is about looking at risk and threats and setting up procedures to answer some specific questions to give a sense of security:

1. What are the real, material risks and threats?
2. What are we doing about them?
3. Is what we are doing actually working?

## RISK MANAGEMENT MODELS

*Companies cannot eliminate all risks for two reasons. First the internal and external threats that cause risk are very dynamic. Second, control investments eventually result in diminishing returns.*[11]

There are quite a few risk management models out there. Just Google “risk management” and you will have, as I did in July 2013, over 388,000,000 results come up. But most of the models concur on a series of steps that make the process viable and effective.

### STEP 1: RISK IDENTIFICATION

Identifying what risks may actually exist in a company’s online infrastructure and digital activity is where it all begins. There are a number of tools to assist the internal risk management professional to complete this on their own, as well as a number of third-party companies that offer auditing and risk assessment services for a price.

[10] “What is Threat? Definition and Meaning,” http://www.businessdictionary.com/definition/threat.html#ixzz2ZsZuuGxr (accessed 2/8/2014).

[11] Nige, The Security Guy Blog, “Security Program Best Practices,” https://nigesecurityguy.wordpress.com/tag/security-lifecycle-methodology/, June 14, 2013.

The gathering and compilation of this information should go beyond a report. It should be looked at as a dynamic and changing set of factors that need to be understood and dealt with in a strategic way, meaning in the best interests of the company (legally of course).

Many companies use a series of security and risk management questions to help guide their collection of the needed data. One good resource is a paperback called *The Ultimate Security Survey* by James L. Schaub and Ken D. Biery. It is in its second edition and a bit on the expensive side ranging from $625 to over $1000 on Amazon.com.[12] But it is very comprehensive.

At a minimum, an audit to gather risk information relating to online and digital activity security should include:

- The mission and demographics of the company
- Inventory of the current online footprint of the company (social media platforms, Web sites, intra and internets, blogs, etc.)
- Inventory of digital and mobile devices accessing company data (laptops, tablets, smartphones, etc.)
- Inventory of access points into and out of company data systems
- Review of current online and digital activity security and risk management strategies and plans
- Review of online/digital employee roles, responsibilities, and liabilities (social media managers, mobile directors, app developers, etc.)
- Review of current IT-related policies and procedures (including social media, IT, privacy, passwords, e-mail, etc.)
- Review of online digital disclaimers and disclosures
- Review of online digital assets (including copyrights, trademarks, trade secrets, content contracts, development contracts, etc.)
- Review of company terms of use and service agreements with third-party vendors
- Review of online and digital content/document retention policies and procedures (including cloud-related legal concerns)
- Review of data collection, data security, authentication, and access
- Review of online crisis and reputation management
- Review of federal and state laws, and industry regulations and compliances that the company is subject to regarding online and digital activity
- Review of human resources' use of online data for the employment cycle (including recruitment, interviewing, performance evaluation, and termination)
- Review of marketing's use of online and digital resources to ensure compliance with specific regulations (such as contest and promotion rules, gaming laws, truth-in-advertising requirements, etc.)
- Review of cyber-risk insurance and coverage

For an example of an audit specifically focused on social media risk and liability, see the Socially Legal Audit sidebar.

[12] Accessed April 1, 2014, http://www.amazon.com/Ultimate-Security-Survey-Second-Edition/dp/0750670916.

## SOCIALLY LEGAL AUDIT®

http://sociallylegalaudit.com

The Socially Legal Audit™ (SLA) tool is an instrument developed by Law2sm, LLC (www.law2sm.com) and Avax Consulting (www.avaxusa.com) to assist a company to ensure that their social media presence and activity is in line with state and federal laws, as well as regulatory compliance.

The audit includes taking an inventory of the organization's social media/digital footprint, interviews with key staff members about social media usage in the firm, comprehensive assessment of legal risks associated with that footprint, and recommended strategies for protection of digital assets and reduction of liability. Components of the audit include:

- Inventory of social media footprint
- Comprehensive report of legal risks/liabilities
- Recommended legal strategies

Audits function as invaluable strategic tool for a company to ensure an ROI in regard to online and digital activity security and risk management. An Ernst & Young commissioned Forbes Insights Global Survey (2012) found that 75% of the respondents indicated that their internal audit function has a positive impact on their overall risk management efforts.[13] In an earlier 2010 survey, 96% of respondents indicate that their internal audit function has an important role to play in their overall risk management efforts.[14]

By asking the right questions, the SLA leads a company to:

- Strategic business insights
- Increased subject matter expertise (specialized knowledge)
- Compliance with laws and regulations
- Decreased liability and risk, including reduction in litigation expenses
- Improved employee–employer relations
- Enhanced customer and brand advocacy relations

Audits are conducted by SLA-certified auditors[15] and reviewed by SLA-trained attorneys who prepare recommendation reports for clients. Training and certification are provided various times throughout the year in various locations around the world.

[13] "The Future of Internal Audit is Now," Insights on Risk, July, 2012.
[14] "Unlocking the Strategic Value of Internal Audit," 2010.
[15] "Certified Auditors—Socially Legal Audit," http://sociallylegalaudit.com/certified-auditors/ (accessed 2/8/2014).

Some information gathering techniques include:

- Brainstorming—a process whereby an individual or a group thinks about a topic or issue and comes up with ideas to solve the problem without filtering them first. The key to this technique is spontaneity. Ideas are reviewed for feasibility later.
- Delphi Technique—a group of experts respond to a questionnaire, their answers are reported back to them anonymously, and they are encouraged to revise their previous answers based on the group's answers. This can be repeated a number of "rounds" or until a consensus is achieved, thereby producing the most "correct" answer.
- Interviewing—a process of asking a specific individual specific questions regarding a specific issue or matter. In the case of online risk management and security, the interviews are usually conducted on key personnel related to the area such as the security director, IT director, as well as some regular staff to understand the breadth of online activity and mobile use throughout the company. In addition, some security and risk management professionals from outside the company may be interviewed to get some insight into the trends and best practices of the industry.

- Root Cause Analysis—a process of evaluating what caused a specific breach or security incident to occur. This takes place after the event but can be used to prevent the event from repeating in the future.
- Checklist Analysis—a tool that lists specific risks that may occur for a specific project or are known to have occurred in other security/risk management systems. The lists can be developed from historical information (prior incidents) and/or knowledge and expertise of current staff.
- Assumption Analysis—a process in which the individual or team documents all the presumptions that they have regarding the issue at hand. These "assumptions" can include things the team believes to be true, which may or may not be true.
- Diagramming Techniques—different processes to visualize data and its relationships by showing them in a sketch, drawing, and/or outline.
- SWOT Analysis—the process of evaluating the strengths, weaknesses, opportunities, and threats of a company's particular security and/or risk management system.
- Expert Judgment—the seeking and use of a decision made by an individual with wide-ranging and authoritative knowledge and/or skill in a particular area after he or she has reviewed and evaluated certain evidence and/or data.

We will be discussing specific risks throughout the rest of the book; however, most online and digital activity risks fall within the following categories:

- IP/Sensitive Data Loss—disclosure or leakage of data that the company defines as proprietary information or confidential information that relates to clients, company strategies, competitive intelligence, etc.
- Compliance Violations—disclosure of information or inappropriate communication of information that violates regulations set forth by federal and state laws and/or regulatory agencies.
- Reputational Loss—one key to successful online activity with clients and the public is transparency of who is communicating and the assurance to the public that it is the company speaking through official company channels. Misperceptions, damaging perceptions, and misinformed assumptions can generate a loss of good will and tarnish a company's name in a matter of characters or minutes due to the prolific and exponential nature of content sharing in the online environment.
- Financial Loss—security and risk incidents can be expensive between the breach itself, the investigation, and remediation strategies put into place, and notification requirements specifically related to leaked data, etc. There have been circumstances where stock prices went down because of a Twitter Tweet. All of the losses on this list can have a monetary consequence.
- Safety Loss—online and digital activity not only leave footprints of where an individual has been but also can provide information as to where an individual can be, whether that is a person or a corporation. This can lead to a physical safety concern for traveling executives and key members of a company's management team, including the board of directors.
- Personal Reputation Loss—online postings may take on a personal nature, indicating specific traits of an individual or describing specific behavior of that individual that may be judged as negative by a company's client base. Concerns here can lead to claims of defamation or damage to a person's character leading to a loss of their livelihood.

## STEP 2: RISK ANALYSIS/ASSESSMENT

> *When asked to name the top three challenges (in regards to risk management) the largest proportion of executives (47 percent) cite difficulty of understanding the entire risk exposure on a global enterprise basis, and nearly as many (44 percent) see the same problem at the business unit level.*[16]

A phrase I like to share with clients is "data that is formatted is information; information that is processed is knowledge; knowledge that is applied is wisdom; and wisdom that is shared leads to success."

A company's list of identified risks must then be put into a risk analysis process to help evaluate the risks in terms of the company's risk aptitude. Greg Chevalier from BlueWave Computing (see BlueWave Computing) calls it a "company's risk appetite." The overall susceptible risk environment is the elephant in the room for many companies, and their key question is "how does one eat an elephant?" According to Chevalier, "one bite at a time." This then leads to the second question, "how much of the elephant does the company want to eat?"

### BLUEWAVE COMPUTING

http://www.bluewave-computing.com/

BlueWave Computing (BWC) was established in 1997 by Steven Vicinanza to provide comprehensive information technology services to small-to-mid-sized companies. Its mission statement reads:

> *BlueWave Computing is the IT management partner of choice for small and mid-size organizations that require the highest reliability and performance from their computing systems but for whom IT is not the core business. We deliver a comprehensive set of IT services that enables them to better achieve their objectives. We do this through highly educated, disciplined, and skilled employees, who aspire to be recognized as the best, and who are passionate about both the technology and the welfare of our clients.*

BWC's business strategy is to have laser-focused solution disciplines within the company to ensure that they can attract the right kind of expertise and build integrity in the market place. One of those focused areas is information security and management, and in 2009 it started the BlueWave Computing Information Security Group. By doing so, BWC expanded its offerings to include information security risk and vulnerability assessments, penetration testing and vulnerability scanning, 7 × 24 × 365 managed security and monitoring that includes intrusion detection and prevention, information security education and training, and implementation of information security technologies. It is also set up to become a leader in information security education with a state-of-the-art training facility and Certified Information Systems Security Professional (CISSP)-compliant curriculum that will allow students to qualify for continuing education (CE) credits.

BWC is a nationally recognized managed service provider (MSP) that has won hundreds of awards and recognition by its peers and security industry associations. They currently have 140 employees, of whom 80% are engineers. They run both on-site and off-site operations for clients and in the security arena offer a "Chief Information Security Officer (CISO) In a Box" that provides the client a comprehensive turnkey solution—risk/compliance, security analysis, network security monitoring—and various complex analytical tools.

This is BWC's competitive edge—offering a one-stop shop for clients from audit to monitoring to compliance. This edge allows the BlueWave client to look at information security in business terms and not just technical terms.

[16] Economist Intelligence Unit (EIU) Global Risk Management Survey, sponsored by KPMG International. https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/risk-management-outpacing-capabilities/Documents/expectations-risk-management-survey.pdf, December 2012.

### INDUSTRY EXPERT: GREG CHEVALIER

President, BlueWave Computing Information Security Group

http://www.bluewave-computing.com/BlueWaveServices.aspx?id=security

Greg Chevalier is currently the president of BlueWave Computing's Information Security Group.

Greg has more than 25 years of experience in the technology field including: 10 years within the IBM Company running a $250 million business unit; 7 years providing executive leadership in growth-stage companies in the $5 million to $100 million revenue range; and 9 years in biometric identification and information security markets including authentication technologies, encryption technologies, and network and wireless access technologies delivered throughout the world.

During an interview, Greg outlined some specific trends he saw in the future regarding information security:

1. Information security risk/advantage must become a front and center strategic decision for companies.
2. Information security and risk management is no longer a percentage of the IT budget but now its own budget with a number of line items, emphasizing its increased importance to the company.[17]
3. Cyber-security insurance is now an option weighed against potential data breaches to offset risk, but will become a standard offering to companies.
4. Within the next decade or so, self-policing of data will regulate privacy concerns as consumers will dictate to companies what data access they find acceptable and companies will adapt to these consumer demands.
5. Wall Street and Financial Analysts will increase their scrutiny of a company's IT security to determine the value of the company's stock and overall value of the company itself.
6. Advanced persistent threats (APTs) will become more evasive and more frequent requiring constant monitoring to detect and remediate these benign but sophisticated data breach attack methods and risks.
7. Mobile makes everything more complex and less controllable as it provides new entry points into a company's data environment. Standards, policies, and controls, and enhanced training will be developed to address mobile risks.
8. Education: it is my belief that information security awareness and education training, along with high-level information security degrees will grow into a national curriculum being pushed down to all levels of our education system—from elementary school to graduate programs.

[17] However, a 2013 Oracle Report found that "for 35% of organizations, their security spend was influenced by sensational informational sources rather than real organizational risks." Brian Pennington, "IT Security Still Not Protecting the Right Assets Despite Increased Spending," http://brianpennington.co.uk/2013/07/17/it-security-still-not-protecting-the-right-assets-despite-increased-spending-2/ (accessed 2/11/2014).

For many companies the answer depends on the risk analysis and the assessment of each risk in terms of:

1. What is the actual risk?
2. What is the probability of the risk occurring?
3. What is the likely impact the risk would have on the company should the risk occur?
4. What will it cost to minimize the risk?
5. What will it cost to remediate the risk should the risk occur?
6. What will it cost to do nothing at all?

Risk Analysis can be done from a qualitative or quantitative perspective and often encompasses both types for a more comprehensive overview of the actual impacts and costs of the risks. Qualitative Risk Analysis looks at the distinctive characteristics of the risk, while Quantitative Risk Assessment is about measuring *the extent, size, or sum of countable or measurable discrete events, objects, or phenomenon*, (of the risk) *expressed as a numerical value*.[18]

[18] "What is Quantity? Definition and Meaning," http://www.businessdictionary.com/definition/quantity.html (accessed 2/8/2014).

Some examples of Qualitative Risk Analysis Tools and Techniques include:

- Risk Probability and Impact Assessment—the process of evaluating the likelihood that a risk may occur and the impact it would have (financially, operationally, etc.) if it does.
- Probability and Impact Matrix—the organization of data divided by columns of categories to highlight potential risks in an easily readable format.
- Risk Categorization—the process of identifying risks by classification and grouping them by those classes to better understand them in relation to the security and/or risk management system.
- Risk Urgency Assessment—the process of identifying and ranking risks by the time range the risk may occur; near-future medium risks may become prioritized over significant risks that may not occur for a year or more.

Some examples of quantitative risk analysis tools and techniques include:

- Sensitivity Analysis—the process of evaluating how a change in a certain factor or system variable can affect the entire security/risk management system. This process allows for a "what-if?" analysis of different results.
- Expected Monetary Value Analysis (EMV)—this process allows you to put a dollar amount on the risk by looking at the likelihood of the risk and the financial impact the risk would have on the company. Each risk can be assigned an EMV, and decisions on priority and handling of certain risks can be made based on the EMV score.
- Cost Risk Analysis—this process focuses on evaluating the risk that certain costs may exceed their initial budgeted amount and, if they do, what the impact would likely be to the system being put into place.
- Schedule Risk Analysis—the process of evaluating certain task durations (in terms of time ranges) and their impact on the system should they not be completed in the time allotted.

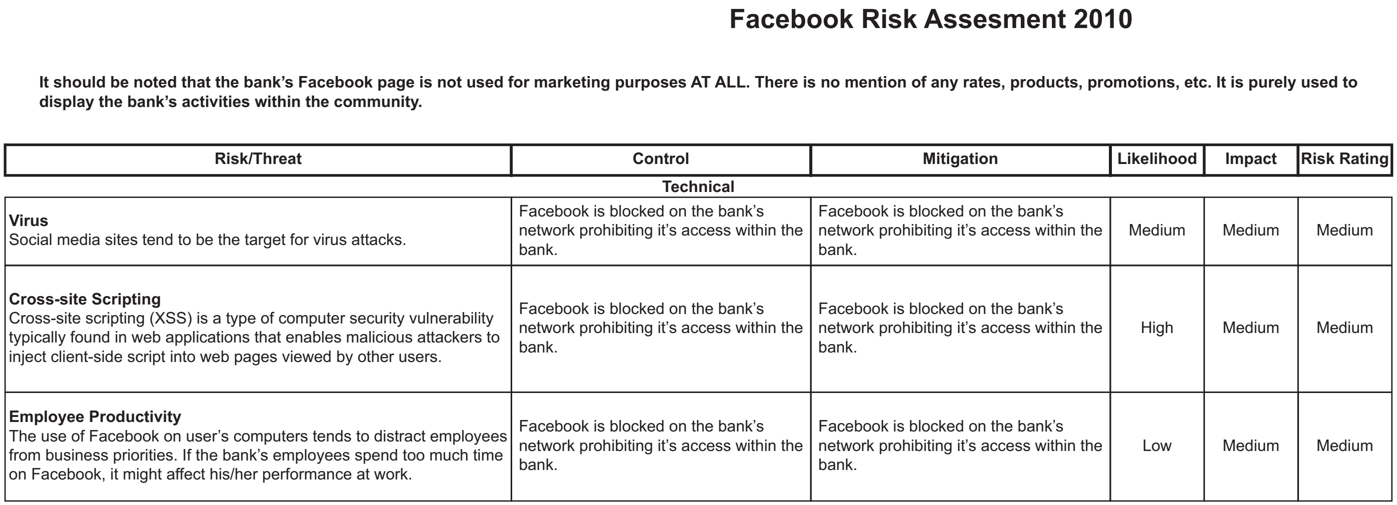
The measurements here focus on time and money, two significant assets for a company, as each can be in limited supply.

Matrixes are common in qualitative and quantitative risk analysis. This way of organizing data gives a comforting sense that everything has a place and is accounted for.

The key to the matrix is the column structure; each column should identify the kind of information being collected and analyzed. Following are two examples of a social media risk assessment matrix structure.

### *Example one*

The matrix example in Figure 1.1 has a simple 6 column structure: Risk/Threat, Control, Mitigation, Likelihood, Impact, and Risk Rating. Likelihood of Occurrence Scales generally flow in an escalating fashion. For example, one scale used in some of these types of matrixes include: *Negligible*, *Very Low*, *Low*, *Moderate*, *High*, *Very High*, *Extreme*; defining these as to whether they may occur between 5 years and multiple times a day. A different matrix may use: *Rare*, *Unlikely*, *Possible*, *Likely*, *Almost Certain*; and defines these as whether they may or may not occur within the next 12–24 months. Some of these matrixes also give each Likelihood level a numeric score, for example, *Rare* is 1–2 and *Almost Certain* is 9–10, that will then be used to give an overall risk rating for the particular risk, threat, or vulnerability. This is a format that can be followed for Impact Severity levels as well. The table below provides an example (Table 1.1).



## Facebook Risk Assesment 2010

**It should be noted that the bank's Facebook page is not used for marketing purposes AT ALL. There is no mention of any rates, products, promotions, etc. It is purely used to display the bank's activities within the community.**

| Risk/Threat | Control | Mitigation | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|---|
| **Technical** | | | | | |
| **Virus**<br>Social media sites tend to be the target for virus attacks. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | Medium | Medium | Medium |
| **Cross-site Scripting**<br>Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | High | Medium | Medium |
| **Employee Productivity**<br>The use of Facebook on user's computers tends to distract employees from business priorities. If the bank's employees spend too much time on Facebook, it might affect his/her performance at work. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | Facebook is blocked on the bank's network prohibiting it's access within the bank. | Low | Medium | Medium |

**FIGURE 1.1 Facebook Risk Assessment Matrix.**

*Copyright © 2013 Jesse Torres. All rights reserved. Used with permission.*

**Table 1.1 Impact Severity Level Examples**

| Example One | | Example Two | |
|---|---|---|---|
| Insignificant | Almost no impact if the threat is realized and vulnerability is exploited. | Insignificant (1–2) | The risk may have almost no impact to financial, operations, compliance, etc. (Enterprise Risk Management - ERM - categories). |
| Minor | Minor effect on the organization that will require minimal effort to repair or reconfigure. | Minor (3–4) | The risk may have a minimal impact to at least one ERM risk category. |
| Significant | Some negligible yet tangible harm that will require some expenditure of resources to repair. | Moderate (5–6) | The risk may have a significant impact to at least one ERM category. |
| Damaging | Damage to the reputation of the organization, and/or notable loss of confidence in the organization’s resources or services. Will require expenditure of significant resources to repair. | Major (7–8) | The risk may have a substantial impact to at least one ERM risk category that will likely require a multi-year recovery. |
| Serious | Considerable system outage and/or loss of customer/business partner confidence. May result in the compromise of services or a large amount of customer/organization information. | Extreme (9–10) | The risk may jeopardize the company’s primary mission and/or solvency. |
| Critical | Extended system outage or permanent closure. May result in complete compromise of services or confidential information. | | |

To calculate a final risk rating, some matrixes will add up the individual numbers of Likelihood and Severity. Example one combines the two factors into a Risk Level Matrix.[19]

| Risk Levels | | | | | | |
|---|---|---|---|---|---|---|
| Likelihood of Occurrence | Impact Severity | | | | | |
| | Insignificant | Minor | Significant | Damaging | Serious | Critical |
| Negligible | Low | Low | Low | Low | Low | Low |
| Very low | Low | Low | Low | Low | Moderate | Moderate |
| Low | Low | Low | Moderate | Moderate | High | High |
| Moderate | Low | Low | Moderate | High | High | High |
| High | Low | Moderate | High | High | High | High |
| Very high | Low | Moderate | High | High | High | High |
| Extreme | Low | Moderate | High | High | High | High |

[19] Jesse Torres, “Sample Social Media Risk Assessment Matrix,” http://www.JesseTorres.com/doc/socialmediaassessment.doc (accessed 02/11/2014).

### *Example two*

This matrix example (Figure 1.2) offers a seven-column structure that takes into account what controls already exist in contrast to what recommended controls need to be implemented. It also allows for specific comments in the matrix itself, such as who is accountable for mitigating the risk, specific details, due dates, etc.

## STEP 3: REMEDIATE

After the initial risk assessment, decisions can be made as to what to do regarding each risk based on their particular circumstances, including their current and projected financial situation. A remediation plan will be developed and put into place outlining the strategies to be implemented to remedy the risk, threat, and/or vulnerability as well as a timetable and budget to ensure that sufficient and appropriate resources are committed to complete the process.

One core set of remediation tools includes the development of a policy and control framework, as well as the drafting and implementation of the policies and controls themselves. Keep in mind that the controls have to make good business sense and align with the company's goals and culture. So the key question is, are the controls being deployed operationally effective?

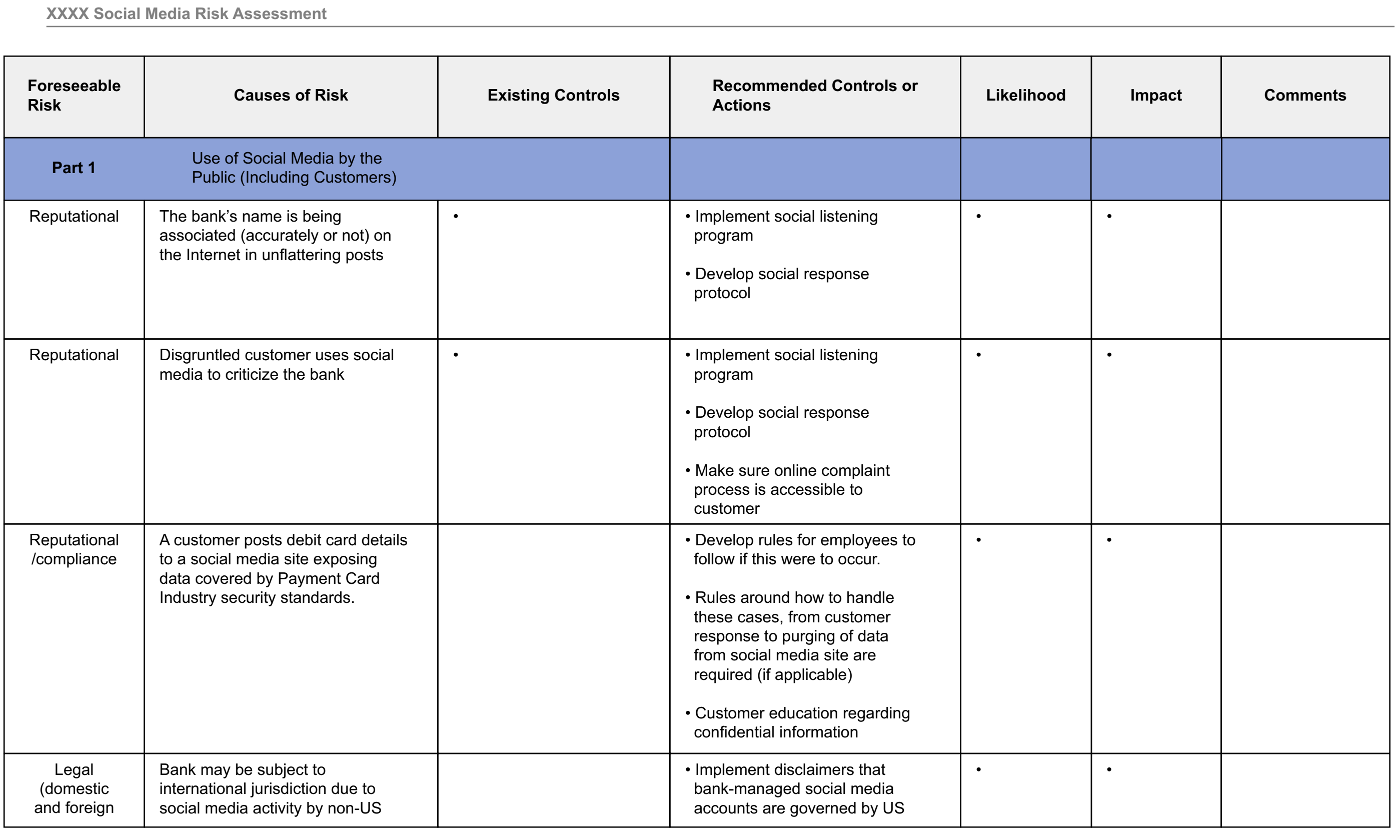
We can surmise that online and digitally related risks can fall into one of four specific categories:

1. Process and procedure
2. Compliance/regulations
3. Policies and controls
4. Technical risks (data, application systems, mobile, networking, etc.)

If these are the categories, the controls and remediation solutions need to align with them. Some of the controls include key information assurance services such as:

- SSAE 16—Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, finalized by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in January 2010.
- SOC 2—Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.
- PCI Compliance—The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.
- ISO 27001 Certification—specifies requirements for the establishment, implementation, monitoring and review, maintenance, and improvement of an information security management system.
- FED RAMP Certification—The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[20]
- Privacy Risk Management—The framework that guides the collection, storage, protection, and use of personal data, including personally identifiable information (PII).

[20] "FedRAMP," http://www.fedramp.gov (accessed 2/11/2014).



XXXX Social Media Risk Assessment

| Foreseeable Risk | Causes of Risk | Existing Controls | Recommended Controls or Actions | Likelihood | Impact | Comments |
|---|---|---|---|---|---|---|
| **Part 1** | Use of Social Media by the Public (Including Customers) | | | | | |
| Reputational | The bank's name is being associated (accurately or not) on the Internet in unflattering posts | • | • Implement social listening program<br>• Develop social response protocol | • | • | |
| Reputational | Disgruntled customer uses social media to criticize the bank | • | • Implement social listening program<br>• Develop social response protocol<br>• Make sure online complaint process is accessible to customer | • | • | |
| Reputational /compliance | A customer posts debit card details to a social media site exposing data covered by Payment Card Industry security standards. | | • Develop rules for employees to follow if this were to occur.<br>• Rules around how to handle these cases, from customer response to purging of data from social media site are required (if applicable)<br>• Customer education regarding confidential information | • | • | |
| Legal (domestic and foreign | Bank may be subject to international jurisdiction due to social media activity by non-US | | • Implement disclaimers that bank-managed social media accounts are governed by US | • | • | |

**FIGURE 1.2 Socially Legal Audit™ (SLA) Social Media Risk Assessment Matrix.**

- HIPAA/HITECH Compliance—Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.[21]
- U.S. Safe Harbor Agreement with European Union (EU)—provides a streamlined and cost-effective means for U.S. organizations to satisfy the EU's directive's "adequacy" standard for privacy protection.[22]
- Data Management—Administrative process by which the required data is acquired, validated, stored, protected, and processed, and by which its accessibility, reliability, and timeliness is ensured to satisfy the needs of the data users.[23]
- Information Technology Internal Audits—address the internal control environment of automated information systems and how these systems are used. IT audits typically evaluate system input, output, and processing controls, backup and recovery plans, and system security.[24]
- Information Technology Governance—The framework of how decisions are made regarding IT Strategic Alignment, IT Value Delivery, IT Resource Management, IT Risk Management, and IT Performance Management.

Many of these control standards require companies to develop and institute various policies in regard to the numerous factors of security risk and management. Policies are basically a statement of intent by a company as to how certain issues are to be addressed by the company and its employees. In many cases, policies also extend to representatives of the company such as freelance or independent contractors, vendors, suppliers, advertising affiliates, etc. Policies list the express rules that will govern certain decisions the company makes and how violations of these rules will then affect employees and those subject to the policies.

Certain policies relate specifically to technology use, and some even outline specific rules for online, digital, and mobile activity by managers, employees, and company representatives. Following is a short list of policies in alphabetical order:

- Blogger Disclosure Policy—this policy lays out guidelines for a company's bloggers to ensure that they reveal their relationship to the company or indicate whether a product/service they are reviewing was a gift from the company being reviewed. This is a requirement from the Federal Trade Commission (FTC) to avoid violation of the false advertising and/or misleading advertising guidelines.[25]
- Bring Your Own Device (BYOD) Policy—this policy outlines specific guidelines and rules employees need to adhere to if they use their own smartphone, tablet, laptop, etc. for company purposes. We will discuss this issue in more detail in Chapter 2.

[21] "HITECH Act Enforcement Interim Final Rule," http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (accessed 2/11/2014).

[22] "Export.Gov—US-EU Safe Harbor Overview," http://export.gov/safeharbor/eu/eg_main_018476.asp (accessed 2/11/2014).

[23] "What is Data Management? Definition and Meaning," http://www.businessdictionary.com/definition/data-management.html#ixzz2a4NPJ1b7 (accessed 2/11/2014).

[24] "Decosimo Accountants and Business Advisors Information Technology Internal Audit," http://www.decosimo.com/www/docs/413.4725 (accessed 2/11/2014).

[25] "FTC Staff Revises Online Advertising Disclosure Guidelines | Federal Trade Commission," http://www.ftc.gov/news-events/press-releases/2013/03/ftc-staff-revises-online-advertising-disclosure-guidelines (accessed 2/11/2014).

- Document/Social Media Retention Policy—here are specific laws regarding document retention, especially in regulated industries. Those laws are now taking into consideration digital imaging systems as a way to preserve the data. Companies may also have their own guidelines as to retaining certain information. This requirement is also extending to social media content, and new applications are offering this capturing of content service.
- E-Mail Policy—this policy outlines the use of electronic communication by employees using the internal company electronic mail delivery system. These policies usually contain prohibitions of private or personal use of the system by an employee.
- Employee Contracts/Agreements with Social Media Clauses—employment letters and agreements are now starting to include clauses that state acceptable and unacceptable use of social media and online activity, and indicating who owns the social media accounts themselves—whether the company or the employee—depending on the account name and the usage of the account.
- Intellectual Property (IP) Policy—this policy outlines the appropriate use of company-owned content: copyrights, trademarks, trade secrets, patents, etc. The IP policy may cover work-for-hire concerns, indicating that anything created by an employee during their scope of employment belongs to the company (including social media posts), as well as logo use on a social media account. We will discuss more on this issue in Chapter 6.
- Information Technology/Computer Use Policy—this policy lays out the guidelines for use of company computer equipment by an employee during their employment period. Certain restrictions, such as secure access to download certain apps, and if devices can be taken off-site, may be included.
- Mobile Device Policy—this policy outlines how mobile devices—tablets and cell phones (whether smartphones or not)—can be used if they are provided by the company or not, if the company does not have a BYOD policy.
- Password Policy—this policy is usually embedded into the computer use policy but it is sometimes helpful to keep separate to emphasize its importance. The policy should lay out the basics of password generation, the importance of why a strong password is a good defense against breach incidents, how often the password should be changed, etc. Considering that most data breaches have a human cause, this policy and the training of employees on all things password related is imperative.
- Privacy/Confidentiality Policy—in the online world, privacy policies usually outline what kind of data is collected and how the party collecting it will use that data. Confidentiality policies remind employees of the nature of certain types of information and the requirements to not disclose specific information to third parties as required for compliance and legal purposes.
- Social Media Policy/Protocols—this policy outlines how employees should use social media whether on behalf of the company or even on personal accounts. The National Labor Relations Board (NLRB) has a lot to say about whether certain clauses in these policies are valid or violate the National Labor Relations Act. Social media protocols are guidelines as to how certain social media posts/comments should be made.

We will review most of these policies in Chapter 4. The key here is to note whether the company has these policies or not and, if they do, are they consistent with each other and do not open up the possibilities of conflicts and therefore leave the company vulnerable to liability.

The SANS Institute also offers a list of 20 Critical Security Controls for Cyber Defense.[26] This list was developed by a group of government and private organizations:

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

*Security involves emotions, beliefs, models of behavior and other non-quantifiable factors which makes the 'how much?' question insufficient.*[27]

## STEP 4: RISK RESPONSE PLANNING

Once the repairs and remediation have taken place, a plan to outline incident response procedures is developed for future reference. This plan will provide specific action steps and reporting guidelines should a breach or other security incident occur. The goal here is to reduce the impact of any specific incident by reducing the time to identify the incident, to locate and contain the incident, to mitigate whatever damage has been caused by the incident, and to institute practices to eliminate the risk of the incident happening again.

A "Risk Register" or "Risk Response Plan" is a good tool to extend the Risk Assessment of Step 2 with the Remediation Process of Step 3. The Risk Register identifies the risks, quantifies the risk score, and then recommends controls and response strategies building a remediation road map based on the company's priorities.

[26] Used under Creative Commons Attribution-NoDerivs 3.0 Unported License from SANS Institute, "The Critical Security Controls," http://www.sans.org/critical-security-controls/ (accessed 2/11/2014).
[27] Jarno Limnell, Director of Cyber Security, Stonesoft, 7/1/2013.

Key Components to a Risk Response Plan (RRP)[28] include:

- List of identified risks
- Definition of who has the authority to act and who can be an owner of a risk to devise and apply the appropriate response
- Results from the qualitative and quantitative risk analysis
- Established responses for each risk
- Expected level of residual risk
- Specific actions required to implement the response
- Budget and timing of each risk response
- Description of any contingency or fallback plans

Based on research, experience, and prior knowledge, there may be a number of options as to how to respond to a particular risk. As the RRP is developed, each option needs to be vetted for feasibility to ensure that it is the best response for the company. Questions to ask to determine the best response option include:

1. What options are there?
2. What constraints are there to the particular project or security implementation?
3. Based on review of the option characteristics, which one offers the most effective way to achieve the business goal?

There are generally four responses to negative risks: avoidance, transference, mitigation, and acceptance. Avoidance is when you change the plan to circumvent the risk all together. It is usually used when the risk is too high and therefore considered unacceptable. Transference is a strategy for when you can shift the risk to another party, such as through insurance, contracts, warranties, etc. Mitigation is when you can reduce the likelihood of a risk occurring or of the damage being unacceptable. Acceptance implies that the risk is considered too low to justify spending any resources on it.

These responses can change during the life cycle of a security project or the company's technology and online activity. Risks that may have been acceptable in the beginning may turn into a risk that needs to be mitigated, and vice versa. The RRP should be a dynamic document and an integral part of monitoring the system (see Step 6).

An interesting note I ran across discusses using an RRP model for evaluating and responding to positive risks or "opportunities."[29] Three response strategies for positive risks are:

1. Share the ownership of the risk with others to ensure you can seize the opportunity.
2. Increase the likelihood of the opportunity coming to pass by enhancing triggers that can set it in motion.
3. Exploit the opportunity by dedicating resources to it, whether in terms of experts or tools.

[28] "IT Project Management: Determining the Most Appropriate Risk Response," http://it-project-guide.blogspot.com/2009/01/determining-most-appropriate-risk.html (accessed 2/11/2014).

[29] "Risk Response Planning by AntiClue," http://www.anticlue.net/archives/000820.htm (accessed 2/11/2014).

On a final note for this section, I would like to mention Bailey and Brandley's *Ten Principles to Guide Companies in Creating and Implementing Incident Response Plans*[30]:

1. Assign an executive to take on responsibility for the plan and for integrating incident-response efforts across business units and geographies.
2. Develop a taxonomy of risks, threats, and potential failure modes. Refresh them continually on the basis of changes in the threat environment.
3. Develop easily accessible quick-response guides for likely scenarios.
4. Establish processes for making major decisions, such as when to isolate compromised areas of the network.
5. Maintain relationships with key external stakeholders, such as law enforcement.
6. Maintain service-level agreements and relationships with external breach-remediation providers and experts.
7. Ensure that documentation of response plans is available to the entire organization and is routinely refreshed.
8. Ensure that all staff members understand their roles and responsibilities in the event of a cyber incident.
9. Identify the individuals who are critical to incident response and ensure redundancy.
10. Train, practice, and run simulated breaches to develop response "muscle memory." The best-prepared organizations routinely conduct war games to stress test their plans, increasing managers' awareness and fine-tuning their response capabilities.

## STEP 5: EDUCATE

Plans and policies may look great on paper, but getting them to be of optimal benefit to the company implies that they have to be implemented effectively. Part of that implementation is the training phrase that should be part of any security and risk management program. The company needs to outline who needs to be trained and what they need to be trained on. A good place to start is on the employee's role in the company and to determine whether they need access to certain information and how they need to access that information digitally and/or via online. However, even though not all employees require access to all company data, there are some basic security issues all employees (including top managers and executives) need to know to keep company data protected and safe.

"Security awareness" training for the general employee population has become an essential component to any security and risk management initiative. It consists of two components: security issues (the content) and adult learning theory (the context). Malcolm Knowles, an American practitioner and theorist of adult education, in the 1970s identified six principles of adult learning[31]:

- Adults are internally motivated and self-directed
- Adults bring life experiences and knowledge to learning experiences
- Adults are goal oriented

[30] Tucker Bailey and Josh Brandley, "Ten Steps to Planning an Effective Cyber-Incident Response," Harvard Business Review, http://blogs.hbr.org/2013/07/ten-steps-to-planning-an-effect/ (accessed 2/11/2014).

[31] "Adult Learning Theory and Principles," http://www.qotfc.edu.au/resource/?page=65375 (accessed 2/11/2014); "Infed.Org | Malcolm Knowles, Informal Adult Education, Self-Direction and Andragogy," http://infed.org/mobi/malcolm-knowles-informal-adult-education-self-direction-and-andragogy/ (accessed 2/11/2014).

- Adults are relevancy oriented
- Adults are practical
- Adult learners like to be respected

Rose McDermott, professor at the University of California, Santa Barbara, gives us a crucial factor to add to this list when the content in the training relates to security and threats. In an interview regarding a paper she wrote for Association for Computing Machinery (ACM) in 2012 entitled “Emotion and Security,”[32] she cautions IT professionals to learn how to train non-IT people. “People will listen to a conversation that is valid, salient, concrete and emotionally engaging. Abstract, pallid, statistical arguments tend to make people’s eyes glaze over.”[33] If you are going to communicate about a threat you should:

- be an expert and a trustworthy source,
- be focused on a specific anticipated attack,
- motivate respondents to act, and
- provide specific concrete actions individuals should take to counter the threat.

In addition to the above, I would like to bring to your attention Ira Winkler and Samantha Manke’s list of seven key elements for a successful awareness program[34]:

1. Get executive-level support from chief officers (C-suite)—this will provide you with additional funding and support.
2. Partner with key departments that have mutual interests and can carry their own level of influence (such as the legal or compliance departments).
3. Be creative in terms of the curriculum and activities; engagement is the key to learning.
4. Make sure to set up metrics beforehand to be able to measure success of the program via change of behavior, attitudes, etc.
5. Educate people about how they can do something instead of just focusing on what they are prohibited from doing.
6. Put your program on a 90-day cycle to ensure information is relevant, current, and reinforced as required.
7. Be multimodal in your program. Use different formats and delivery methods to spread the message of security awareness—from online games and apps to traditional newsletters and posters—offering something for everyone.

Connecting those seven factors, Ira continues: *The mere act of providing a set body of knowledge does not change behavior. Information must be provided in a way that relates to how employees think and behave. There must be a personal association of how the knowledge would impact their actions. There is also a difference in providing an individual information on a one time basis, and delivering information in different formats over the course of time to effect change.*[35]

[32] “Communications Magazine of the ACM,” Vol. 55, No. 2 (February, 2012), pp. 35–37.

[33] “Ignoring Security Advice from the Pros: The IT-User Disconnect—TechRepublic,” http://www.techrepublic.com/blog/it-security/ignoring-security-advice-from-the-pros-the-it-user-disconnect/ (accessed 2/11/2014).

[34] “The 7 Elements of a Successful Security Awareness Program—CSO Online—Security and Risk,” http://www.csoonline.com/article/732602/the-7-elements-of-a-successful-security-awareness-program (accessed 2/11/2014).

[35] “7 Reasons for Security Awareness Failure—CSO Online—Security and Risk,” http://www.csoonline.com/article/736159/7-reasons-for-security-awareness-failure (accessed 2/11/2014).

## STEP 6: MONITOR

*The three certainties of life: Death, Taxes, and Getting Hacked.*[36]

Having done a risk assessment once does not mean you are finished. Continuous monitoring involves the identification, analysis, planning, and tracking of new risks, constantly reviewing existing risks, monitoring trigger conditions for contingency plans, and monitoring residual risks, as well as reviewing the execution of risk responses while evaluating their effectiveness.[37] Various tools used to accomplish this daunting task include:

- Risk Audits—the process of investigation, evaluation, and assessment of the actual, perceived, and projected risks that a company may face. These audits can be performed by an internal company professional or an external third party or company.
- Variance Analysis—this process looks at what was projected to occur and what actually occurred, whether financial (budget targets) or operational (performance goals), as well as the causes of the differences between the two.
- Trend Analysis—the evaluation of information from a designated period of time of a specific factor to identify patterns and relationships between factors and to use that data to project what may occur in the future.
- Technical Performance Measurements—reviewing specific indicators that the company has identified to determine whether the strategies and/or tools being implemented are achieving the desired results.
- Reserve Analysis—the process of reviewing the physical and financial status of equipment, tools, and other resources relating to the online and technology activity of a company, including costs to repair and/or replace those resources.
- Status Update/Review Meetings—risk management and security strategies need to be reviewed and the RPP and other risk management/security documents updated. It is important to keep the security and risk management teams up to date on any incidents that may occur, the response to the incident, new tools available for responding to incidents, new trends in security concerns, etc.

Keep in mind that if you set up policies as part of your controls, you need to ensure that you are enforcing them. Periodic policy reviews and enforcement reviews will provide you with data to determine whether the policy implementation has been successful or not.

*Corporations will spend around $68 billion worldwide this year on IT security measures including firewalls, network monitoring, encryption and end-point protection.*[38]

[36] James Christiansen, “The Three Certainties of Life: Death, Taxes, and Getting Hacked | ID Experts,” http://www2.idexpertscorp.com/blog/single/the-three-certainties-of-life-death-taxes-and-getting-hacked/ (accessed 2/11/2014).
[37] RobustPM Home page, http://www.robustpm.com.
[38] Kyle Marks, “The Most Overlooked Part of Your Data Security,” Harvard Business Review, http://blogs.hbr.org/2013/06/the-most-overlooked-part-of-yo/ (accessed 2/11/2014).

## STEP 7: RESPOND

Keep in mind that what hackers are usually after with a breach is the data and not necessarily the device the data was on. The device serves as an access point, a critical one that needs to be watched and protected.

When responding to an incident, the goals are simple: limit the damage; increase the confidence of external stakeholders; and reduce recovery time and costs.[39]

Responsiveness to an incident focuses on time. The basic stages of a breach include:

- Incursion—the moment the unauthorized enters the system
- Discovery—the period of time the unauthorized takes to map out the system and discover where the data is
- Capture—the stage where the unauthorized commandeers the data using root kits or other tools at their disposal
- Exfiltration—when the data is sent back to the unauthorized; data is not necessarily removed from the system but copied to another location[40]

These stages present three critical points for responding to the incident to mitigate the damage and repair the breach:

- From the point of entry to the compromise
- From the compromise to discovery by the company
- From discovery by the company to remediation

An incident response team with specified members is a must and should be summoned as soon as an incident is discovered. Each member of this group should have and understand his or her role in the upcoming investigation and the remediation of the damage. Internal company members to this elite group should include representatives from the following departments:

- IT Security
- IT Operations
- Data Collection and Monitoring Division (if applicable)
- Physical Security
- Human Resources
- Legal Department
- Compliance Department
- Public Relations
- Management/Executive Level

In addition, third parties or individuals from outside the company may be called in an advisory role to the team and to ensure objectivity in terms of development and implementation of security and risk management systems.

[39] Bailey, Tucker and Josh Bradley, Harvard Business Review Blog, “Ten Steps to Planning an Effective Cyber-Incident Response,” http://blogs.hbr.org/2013/07/ten-steps-to-planning-an-effect/, July 1, 2013.

[40] Blue Wave Computing Panel Discussion on “The World of Information Security,” June 18, 2013, Gwinnett Technical College, Georgia.

## BEST PRACTICES FOR INCIDENT RESPONSE

- Devote time to incident response planning before something bad actually happens. The millions saved by avoiding a breach justify the money spent on planning and preparation.
- Make sure your incident response team has the appropriate skills to deal with an incident, both technical and soft—such as being able to maintain calm, reduce panic—can mobilize individuals to take appropriate action, and effectively communicate with executives, the media, and employees.
- Do dry runs of the incident response to catch unanticipated obstacles and to ensure the response is appropriate.
- Make sure your incident response team is trained on how to identify and preserve physical and digital evidence.
- Determine the facts of the incident: what data was involved, was the data encrypted, the timeline of the incident, etc. It is important to get all the details before you notify or make an announcement of the incident, especially to the press.
- Make sure the message you do decide on is consistent across the board—from internal to online to clients to media to stakeholders. Determine who will be the point person for incoming calls and how the calls will be handled.
- Practice customary examination techniques such as interviewing the relevant individuals related to the incident and conducting technical and forensic investigations.
- Prepare to notify, and then actually notify, as required based on state and federal laws governing data protection and privacy. Record the incident in appropriate logs and registers, including remediation solutions and outcomes.
- Plans need to be reviewed and revised to keep up to date at least annually, and especially after an incident has occurred. Reinforce employee awareness of security.

## BONUS: TEN IT SECURITY MYTHS

It is interesting what we in the security field believe when it comes to security, risk, and our own companies and capabilities. The following table outlines Ten IT Security Myths compiled by various online posts by various IT security professionals (Table 1.2 ). Do any of these ring true to you?

**Table 1.2 Ten IT Security Myths**

| | Myth | Comment |
|---|---|---|
| 1 | I'm an IT professional, it won't happen to me. | No one is infallible, and it is those of us who practice in this area that sometimes have a "God complex" and are most susceptible to cutting security corners. How strong are your passwords? |
| 2 | We have backups and backups. We are OK. | When was the last time you verified the data on the backups and made sure that the backup system was doing what it is supposed to do? |
| 3 | This system is secure. I implemented it. | How long ago was it implemented? Have there been any changes to the systems such as additions of access points for mobile devices? Probably time to review. |

*Continued*

**Table 1.2 Ten IT Security Myths—cont'd**

| | Myth | Comment |
|---|---|---|
| 4 | We detected the incident 5 min ago. We don't know what caused it, but we have it under control. | Really? How do you know? Who are you telling this to? Will you have to take any of this statement back? |
| 5 | We are not a target. Our data is not important. | But your data connects with client data and other data that can be very important and very valuable to the criminally minded or just a disgruntled employee. |
| 6 | Compliance is security. | Compliance sometimes is just paperwork. It can serve as a starting point for a comprehensive security and risk management system, but it should not be the final checkoff. |
| 7 | We've got the latest and greatest in information security and risk management tools. We are safe. | Software, policies, USB keys, etc. are all great—but don't forget the human element. According to security expert Jack Daniel: "Having the right people is more important than having the right tools. And that requires hiring the right people, investing in them, and retaining them—three processes we often get wrong."[41] |
| 8 | We have a firewall. Our data is secure. | Randy Rosenbaum, executive partner at Alert Logic, stated in a recent technology forum that "Breaking into a firewall you can learn with 20 minutes of YouTube."[42] Firewalls may slow a hacker down, but it does not stop the attack from coming. |
| 9 | Any and all vulnerabilities need to be addressed as a priority over business operations. | Even though security and risk management is considered a strategic business concern, it should not overtake the primary purpose of the business being in existence. Careful risk analysis, including financial considerations, must help guide decision making as to where the risks and remediation fit into the larger picture of the business acumen. |
| 10 | Security people know their stuff and business people just need to listen and give the money. | One of the key concerns in security and risk management is the dialogue between IT security personnel and upper management—a lot seems to get lost in the translation from technical to strategic. Security needs to be able to speak the business language to justify the funds it is requesting. |

## SECURITY/RISK MANAGEMENT APPS

Here is a table of some of the risk management and security-related apps available for current digital and mobile devices (Table 1.3). Security apps will be discussed in Chapter 2 as they focus on securing and protecting mobile devices, and not enterprise security. New apps are constantly being developed, so periodic searches to see what is new in the market is recommended. Each application has pros and cons, and you should evaluate each (as well as have your security and risk management team review) before selecting it to download and/or purchase.

[41] David Spark, "Top 25 Influencers in Security You Should be Following | the State of Security," http://www.tripwire.com/state-of-security/security-data-protection/top-25-influencers-in-security-you-should-be-following/ (accessed 2/11/2014).

[42] The World of Information Security, Gwinnett Technology Forum, June 18, 2013, Georgia.

**Table 1.3 Security/Risk Management Apps**

| Name | Compatible Devices | URL | Price |
|---|---|---|---|
| Citicus MOCA | iPhone, iPad, iTouch | http://www.citicus.com/citicusmoca.asp | Free |
| Citicus™ Limited: Risk Assessment Checklist Mobile App | iPhone, iPad, Android, Blackberry Playbook, Windows Mobile | http://www.citicus.com/citicusmoca.asp | Free |
| Canvas: Risk Report | iPhone, iPad, iTouch | http://www.gocanvas.com/mobile-forms-apps/3257-Risk-Assessment-Checklist | $2.99 |
| Risk Management Services: Breach Support | iPhone, iPad | http://www.risk-management-services.biz/Risk_Report.html | Free |
| Strategy and Risk Studio | iPad | http://strategyriskstudio.com | $25.99 |
| Risk Calendar Chart Tool | iPhone, iPad | https://www.quixey.com/app/2400208252/risk-calculator-chart-tool | $.99 |
| Marsh Risk Management Research App | iPad | http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch.aspx | Free |
| SG Risk Log | iPad | http://www.simplegeniussoftware.com/sg-risk-log-ipad.html | $9.99 |