Rodney F. Davis

Incorporating Cyber Risks into the Enterprise Risk Management Strategy

Once the overall Objectives, Goals, Strategy, and Measures (OGSM) have been established for a firm or organization as part of the strategic planning process, the real work commences to begin monitoring the progress towards OGSM along with the intent of maintaining a competitive economic edge and increased profitability. During this monitoring, risks are deferred, mitigated, transferred, or tolerated\accepted based on the risk appetite of the firm and the overall Enterprise Risk Management Strategy.

In theory, all three communities of interest (IT, Business, and Information Security) should be fully engaged in defining and monitoring the overall Enterprise Risk Management Strategy. While IT has been able to gain the attention of decision makers over time, Information Security must become incorporated into the OGSM process as well. This incorporation must be conducted by clearly defining information security risks that will impact the firm without over complicating threats and vulnerabilities related to cyber-attacks. The overall goal of *Information Security* is to protect the company's assets; the overall goal of *Information Security Management* is to communicate the utmost importance of protecting the company's assets by understanding the OGSM of the firm or organization and effectively translating cyber risks into terms that can be understood by the business partners and ultimately the C-Level. In general, the Information Security Manager should be able to articulate the linear relationship between scenarios, cyber risk events and incidents, causes, and business impacts. These cyber risk events should focus on strategy, protection of the company's assets, and education and awareness.

Strategy and Goals-Winning is Everything

Simply put, organizations create strategies in order to win – business from competitors, talented staff, and customer satisfaction. Sustainable success for strategies is accomplished by the creation of specific goals. Objectives are the tactical components that underlie the goals. Over the years, companies have gotten better with identifiying operational risks that can jeopardize the long term strategy. For the most part, identified risks are related to staffing and resources, the ability to compete in the marketplace based on technology capability, and adherence to regulatory mandates both known and unknown. While these are valid risks that all companies face regardless of industry, the protection of information tends to get overlooked in many cases. Discussions take place regarding the protection of information however, this topic tends to take a bottom up approach. Unfortunately, the bottom up approach of reporting risks related to information protection isn't always successful as the message or need never makes it to top management and ultimately the board.[1] It is for this reason that the information security manager (i.e. CISO) should always be involved in the strategy sessions to ensure that the protection of information is embeded into the overall organizational strategy. Without an *information security* strategy in place to protect the data, knowledge, and content related to *organizational* strategy, the long term vision will be short lived.

---

[1] Whitman, Michael, E, Mattford, Herbert, J. Management of Information Security 3rd Edition, (Cengage Course Technology 2010) page 54

Overall, information security should provide safegaurds to protect the confidentiality, integrity, and availability of an organization's information. As goals and objectives are created by senior management, risks related to information security should be addressed.

Protecting the Company's Greatest Assets (People and Information)

To prevent the disruption of business processs and to ensure that the organization's critical systems remain available, the Information Security Manager must ensure that proper staffing levels are distributed across different, geographic locations and critical systems are consistently backed up and tested in disaster recovery scenarios. These two topics (Business Continuity and Disaster Recovery) will require the Information Security Manager to not only work closely with the Business Community team to ensure adequate staffing levels exist across the organization, but to also work closely with IT to make sure that systems are available at all times based on their criticality rating. In many instances, the Information Security Manager will need to convey the importance of Business Continuity and Disaster Recovery testing with outside suppliers and application service providers (ASPs) as well. Each of these tasks (Business Continuity testing for the organization, Disaster Recovery testing for the organization, and Business Continuity and Disaster Recovery testing for an organization's suppliers and ASPs) will require the Information Security Manager to influence and provide direction without necessarily having control. All of these items directly impact the organization's risk management strategy as well as objectives, goals, strategy, and measures for the overall organization.

When influencing the business community to adhere to business continutiy testing, the Information Security Manager must provide scenarios that paint a picture for the business. In many cases, the business area is aware of the risk of not having adequate staffing, however many times the message has to be reinforced. Business disruption can lead to missed service level agreements for both internal and external customers.

In some instances, business areas may be able to leverage other geographic locations to distrbute work. These geographic locations should be in different timezones in order to be effective. Additionally, a business impact analysis should be created to identify the business processes with the highest potential of business disruption [2]. The Business Continuity function and oversight usually resides in the Risk Management area of an organization. There are also Business Contiuity representatives embedded in business areas to coordinate call tree testing and business process testing. The Information Security Manager can ensure that business continuity gains the proper attention at the management layer of an organization by focusing on the following topics based on a very insightful article written by Rama Lingeswara Satyanarayana Tammineedi, CISA, BCCE, CBCP, CISSP, PMP in the 2012 Volume 1 version of the ISACA Journal [3]

[2] Business Continuity Planning http://www.ready.gov/business/implementation/continuity – accessed July 2013

[3] Tammineed, Rama, Key Issues, Challenges, and Resolutions in Implementing Business Continuity Projects, ISACA Journal, Volume 1, 2012 http://www.isaca.org/Journal/Past-Issues/2012/Volume-1/Pages/Key-Issues-Challenges-and-Resolutions-in-Implementing-Business-Continuity-Projects.aspx –accessed July, 2013

- Senior management commitment and involvement
    1. Delegation By Senior Management
    2. BCM Implementation for the Wrong Reasons
    3. Business IT Disconnect
    4. Technology-Only Approach Toward Resilience
    5. Lack of Consensus Between Senior Management and Operations Management
    6. Absence of a single BCM Framework Across Multiple Offices
- Lack of thorough understanding of the data dynamics and dependencies involved in data recovery by BCM practitioners
    1. Incomplete Understanding of Data Recovery Elements
    2. Failure to Consider Full Recovery
- Inappropriate approach in executing BCM processes
    1. Location Based Risk Assessments
    2. Equal Weight Assigned to All Risk Attributes
    3. Inappropriate BIA Approach
    4. Challenge in the Deployment of a BCM Tool
- Incorrect and/or inappropriate assumptions in formulating business continuity and disaster recovery plans
    1. Failure to Consider All Relevant Assumptions and Limiting Factors

Disaster Recovery testing involves coordination with IT in order to keep business critical systems available. The planning aspect of disaster recovery (i.e. disaster recovery planning), initiates when the clock is ticking to get critical systems back on line[4] - this is where IT involvement is absolutely crucial. While planning for the possibility of a disaster occurring, the business areas should be able to articulate which systems should be brought back on line first. The Information Security Manager can add value to this planning by ensuring that the proper RTO (Recovery Time Objectives) are identified by the business area.

In disaster recovery planning there are two challenges that normally take place in organizations. The first challenge is determining which systems are most critical and capturing accurate recovery time objectives for the business. For example, there may be several applications that the business may feel are critical; however, they are only used sparingly. The Information Security Manager, along with IT should be able to convey the message that inaccurate recovery time objectives can be costly as numerous resources will be dedicated to bring a system back on line in a certain time frame. A second challenge in disaster recovery planning occurs in IT. Specifically, when multiple applications of varying critically are located within the same infrastructure. An example of this would be if a non-critical application is located on the same server or infrastructure as a critical application. IT will focus on recovering the critical application and, by default; the non-critical application will be recovered as well. This results in wasted valuable time and lack of focus on other critical applications with short windows of time for recovery time objectives. This is not a business problem; instead it is an application hosting problem that should be resolved by IT. In terms of the Information Security Manager's role in this scenario, guidance and direction will need to be administered to ensure that IT doesn't host applications with varying recovery time objectives on the same servers and infrastructure. Also, as a valued business partner, the Information Security Manager should ensure that the business community is aware of this issue. This scenario can also

[4] Harris, Shon, Business Continuity and Disaster Recovery, Chapter 8, page 887, CISSP All-In-One Exam Guide 6th Edition

cause regulatory ramifications if certain systems are not available based on poor design in the Disaster Recovery Planning process. If an investor's check is not process and mailed, or if critical patient data is housed on a system that contains non-critical information, there could be fines, and ultimately the organizational would suffer reputational damage. As stated in the ISACA Journal's 2002 Volume 1 issue by Yusufali F. Musaji, CISA, CGA, CISSP titled 'Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans', '*Business Continuity and disaster recovery are so vital to business success that they are no longer remain a concern of the IT department, alone.*'[5]

Another facet of disaster recovery that is seldom discussed is coordinated testing with suppliers and vendors. Since suppliers and vendors are an extension of an organization's processes, it makes perfect sense to occasionally conduct testing to ensure that processes are uninterrupted between the organization and the suppliers and vendors. The Information Security Manager should ensure that a robust supplier governance program is in place within the organization to provide oversight of vendor and supplier service level agreements and metrics. Also, the Information Security Department should administer periodic risk assessments on vendors and suppliers and also conduct regular site visits to the location(s) of the suppliers and vendors with the business.

With regards, to protecting the company's greatest assets, the Information Security Manager will need to use subject matter expertise and real world examples to explain the risk of not complying with business continuity and disaster recovery testing along with the potenial impacts to the organization.

Education and Awareness-Everyone is Responsible for Information Security

It is often said that the responsibility of the protection of information falls soley on the shoulders of the Informaton Security Department. While it is true that the primary role of maintaing the confidentiality, integrity, and availability of data belongs to Information Security, security engineers, and practitioners, the Information Security team cannot be everywhere all the time to ensure that all vulnerabilities in the organization are mitigated. Frankly, information security is everyone's responsibility and this accountability can be enforced by effective education and awareness for the business community. The Information Security Manager must be able to convey the message that the entire organization is responsible for protecting the assets that are critical to the organization's success.

In many instances, when an information security related event occurs, the IT and Business Communities of Interest tend to fault the Information Security team. However, end users are steadily becoming a common cause for information security related events[6]. What the Information Security Manager must continually convey is that, although Information Security maintains and monitors networks and devices to ultimately protect company data, the risk ownership belongs to the business area. Information Security is a cost center, or a practice, that supports the

---

[5] Musaji, Yusufali, F Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans, ISACA Journal, Volume 1, 2002. http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/Disaster-Recovery-and-Business-Continuity-Planning.aspx – accessed July, 2013

[6] Miscellaneous, Security Liability, Who's To Blame for a Data Security Breach, http://searchsecurity.techtarget.com/Security-liability-Whos-to-blame-for-a-data-security-breach – Accessed July, 2013

organization. The business is ultmately responsible for any data breaches or information security related events that jeopardize the company. It is for this reason that everyone in an organization should understand information security risk. There will always be subject matter experts related to information security, however, it is the responsibility of the Information Security Manager to ensure that the ownership of risk is communicated in management circles and socialized throughout the organization.

Even with effective training, incidents will occur, however they will be significantly mitigated with good user training and communication. It also important to stress the fact that, without 'encouragement' from senior management, training will become a check the box initiative for many people. Therefore, it is crucial to have management buy in for any training initiatives.

One of the simplest and most effective (in terms of impact and cost) ways to adminster security and awareness is through an information security calendar or posters. There are several resources on the web that offer free calendars and posters[7]. With the exception of printing costs, these resources are a great way to promote the message and importance of information security. Again, as previously mentioned, obtaining management support and budget will ensure that this message and importance are enforced. In addition to calendars and posters, infographics are gaining popularity in the education and awareness space. Infographics allow users to quickly obtain knowledge about a topic through the use of colorful graphics, various fonts, and direct messages with alarming statistics.

Along with effective education and awareness, adherence to information security policies can ensure accountability in the user community; however the policies should be easy to undersand and applicable to real world incidents. This way users will be able to immediately act when the incident occurs, or they will quickly recollect a point in time when the incident previously occurred and they did not take the appropriate action. According to the third of the Ten Commandments of Information Security Awareness and Training *'If they cannot see it, they will not learn it.'* [8]. One of the most efficient ways to administer any type of training is with an example that can be visualized. It is also proven that visual learning is more effective[9]

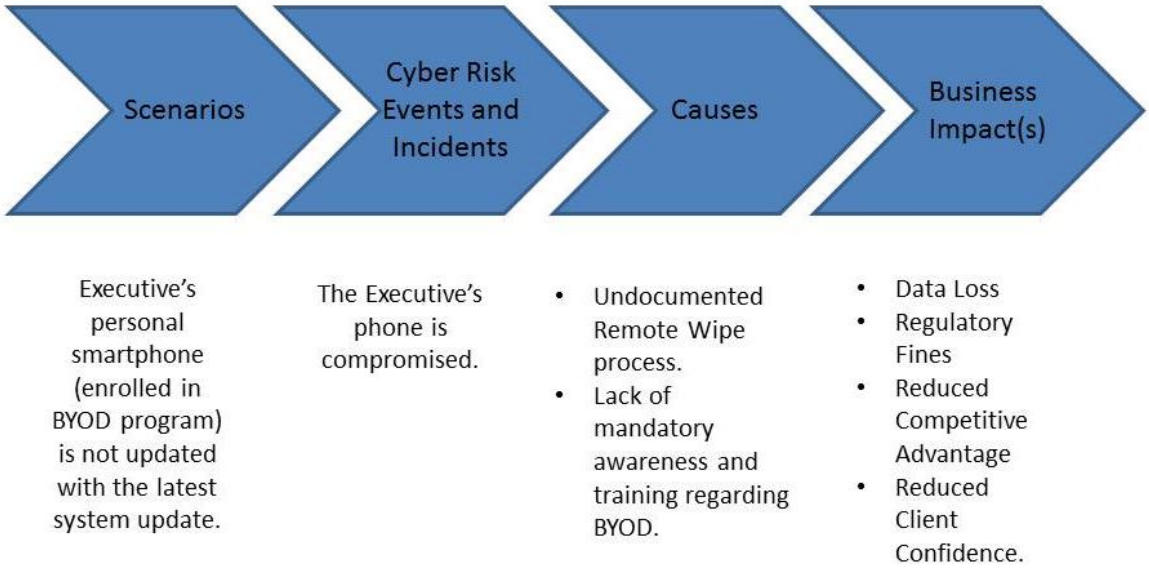
The image below depicts an example of how a real world information security risk can ultimately impact the business. This particular scenario is based on a bring your own device (BYOD) related risk. This example will allow users to see, step by step, how not keeping your personal communication device updated with the latest updates can directly impact the business while it is enrolled in a BYOD program. The communication flow should transform from an information

[7] Native Intelligence, INC Free Information Security Awareness Calendars, Posters, and Tips, http://www.nativeintelligence.com/ni-free/ni-free-posters.asp - Accessed July, 2013

[8] Desman, Mark, B, The Ten Commandments of Information Security Awareness Training Information Systems Security, January/February 2003 page 39-45

[9] Visual Teaching Alliance http://visualteachingalliance.com/ Accessed July, 2013

security incident, to business impacts.



With 72% of organizations now allowing BYOD options for employees[10] this risk will continue to proliferate.

This same type of communication flow can also be created for various other information security related scenarios that user's initiate (either intentionally or by accident). These scenarios include[11]:

- **Social Media**: Sensitive Information posted to LinkedIn, Twitter, and Facebook information can be shared with the world in *seconds*.
- **Texting\Instant Message**: This type of communication usually occurs rapidly with little thought used in regards to content.
- **App Downloads**: App downloads on Blackberries, iPhones, and iPads should be monitored, specifically on BYOD enabled devices. Users should also be mindful of downloading applications on company owned devices as well.
- **Cloud Based email\drop boxes**: Convenience over security will not be a good outcome.
- **Passwords:** Users are still using 'basic' passwords.
- **Lost Devices**: Small devices with large storage become lost or misplaced: the result is exposed, sensitive company data.

In many organizations, each employee is held accountable for protecting company information and complying with the standards, procedures, and policies related to Information Security. Risks that can negatively impact an organization due to non-compliance include:

- Reputational Risk
- Data Breaches
- Financial Losses

---

[10] George, Trosten, PHD Mobile Risk, Bring your Own Device Data Breach http://www.isaca.org/Journal/Blog/default.aspx accessed – July, 2013

[11] Ferrara, Joe, Top 7 End User Priorities http://www.scmagazine.com/top-7-end-user-security-priorities-for-2013/article/274058/ accessed – July, 2013

- Regulatory Sanctions
- Legal Sanctions

Any risk listed above has the potential to derail an organization's strategy. Therefore it is important for the Information Security Manager to ensure that Senior Management is aware of Information Security training that should occur throughout the organization.

There are traditional security and awareness topics that every Information Security Manager should ensure that their organization is aware of. Following is a subset of topics that the Information Security Manager can ensure organization wide focus on. These topics include:

1. **Information Classification**: Users should know how to distinguish between Confidential, Public, and Internal related data.
2. **Password Maintenance**: Passwords should be changed every 60 days; avoid using words from the dictionary; include upper and lower case letters; use digits.
3. **Mobile Device Security:** Keep your laptop locked when docked; ensure your laptop or mobile device is never left unattended.
4. **Appropriate Use of Social Media*:** Do not share company information on social media sites.
5. **Phishing**: Avoid 'urgent' emails asking for help or money; never provide your password.
6. **Internet Usage**: Users should understand that all web usage history is logged. If it isn't, then it should.
7. **Appropriate Use of Email**: Users should not send company information to their personal email accounts.

**In many organizations, Marketing teams use Social Media to reach out to their customers. Specific training should be provided to Marketing teams to ensure that appropriate information is shared. Also, the Legal and Compliance areas should vet all information published by the Marketing areas of an organization mitigate additional regulatory scrutiny.*

Conclusion

In theory, the harmonization between the three communities of interest should encourage top down decision making along with healthy debate. Unfortunately, based on operational reality and well documented concerns captured in the *Governance of Enterprise Security: CyLab 2012 report published by Carnegie Mellon University*[12], gaps still exist in terms of senior management and board level oversight of activities related to cyber risks. This can easily translate in to risks that threaten the objectives, goals, strategies, and measures of an organization.

While it is important to understand the technical risks based on security architecture and design, encryption, and the current list of cyber threats, the ability to translate these risks into business impacts at the top of the house is absolutely crucial. This emphasizes the importance and value of Information Security Management to provide direction and subject matter expertise when appropriate. Without this understanding and effective communication from the top down,

[12] **Governance of Enterprise Security: CyLab 2012 Report How Boards & Senior Executives Are Managing Cyber Risks Author: Jody R. Westby** http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf

Information Security will always remain in a silo; and out of the purview of the C-Suite and, more importantly, the Board of Directors. This ultimately puts firms and organizations at risk.

Translating cyber risks into business impacts is more of an art than a science and an essential skill set for the Information Security Manager to master. Without addressing this critical translation, there will always be a disconnect throughout the organization. As technology becomes more complex, and as risks increase with information sharing around the globe, everyone should have a clear understanding of the potential business impacts to adjust the OGSM plan accordingly to mitigate risk. The Information Security Manager is a key player in facilitating this understanding.