GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

The Evolving Role of Security Structures

GIAC (GSLC) Gold Certification

Author: Dale Emel, dale.emel@gmail.com
Advisor: Dr. Kees Leune

Accepted: January 26th 2010

Abstract

Current economic and political conditions are changing the environments businesses operate in. Depressed economies have increased threats to intellectual property (IP) and data, while networks and technologies designed to increase opportunities have multiplied threat vectors and vulnerabilities.

"2009 represents the largest collection of data loss on record, the majority of loss stemming from a single credit card processing source" (Greenberg, 2009)

As companies adopt new technologies to grow revenue and identify new markets, security organizations, large and small, need to address risks through a management structure that embraces data protection, governance, and collaboration. Security has never been better positioned to become a strategic part of the business and can demonstrate that in 2010 and beyond.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

1. Introduction

With falling budgets and escalating threats, firms and corporations are examining new methods and approaches to gaining strategic and competitive advantages through viral growth and lower operating costs. As CEO's and Boards of Directors look to enhance their businesses', increased threats and restrictions have drawn their attention to improving their positions in corporate risk management and regulatory compliance. This thinking presents new opportunities and challenges for security professionals and leaders.

This paper examines some of the most popular strategies businesses are using in 2010 and suggests extensions and additions to the security management structures covered in the SANS Management 512 course, *Security Leadership Essentials for Managers* (The SANS Institute, 2009). My research began by examining the competitive business market trends in 2009 and those planned for 2010. Results demonstrate that the business trends for 2009 will continue into 2010 with a strong focus on Social networking, Cloud Computing, and the Consolidation of resources and systems to reduce costs.

Combined data from Baseline (Greengard, 2009) and PriceWaterHouseCoopers (PriceWaterHouseCoopers, 2009) illustrates the areas of investment that businesses are planning to focus on in 2010 (Figure 1 - *Planned areas of Investment for 2010*). Survey respondents revealed that Green Initiatives (92% of the respondents), Centralization (76%), Social Knowledge[1], Cloud Computing, and Hardware Infrastructure upgrades would dominate the investment focus (note percentages do not equal budget allocations). These initiatives are introducing new technologies, new processes, and

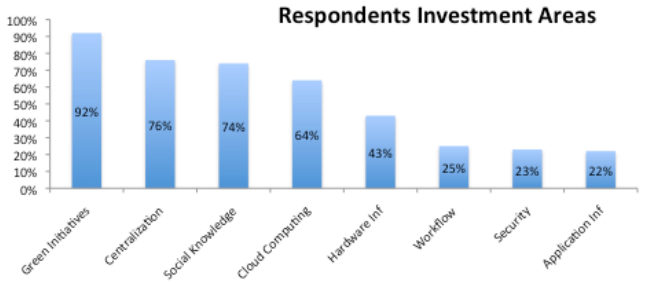


Figure 1 – Planned areas of investment for 2010

[1] Social Knowledge is defined as the use of Social Networking to foster Customer Interactions, Feedback and Knowledge sharing

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

additional revenue streams for businesses, along with introducing new concerns, such as increased exposures to risk, regulations, and unknown threats. More importantly, and the point of this paper, is that these initiatives are introducing new opportunities for security organizations to become strategic partners to the business by adopting a data protection, governance and collaborative mindset.

Why advocate for change in security management structures? Because today businesses are in the middle of the worst economic downturn in more than thirty years and their survival depends on being more competitive and more efficient than ever before. This means businesses are moving at a rapid pace, deploying new services and products faster than ever before, and consequently exposing more corporate data than at any other time in recent history. For instance, **222,346,827** data records were compromised as of Dec 2009 (Identity Theft Resource Center, 2009). The good news in this number is that the number of breaches actually went down (meaning security is working); the bad news in this number is that we (security) seem to be more focused on securing the enterprise than securing the actual data (Figure 2 – *Cost of a Data Breach*).

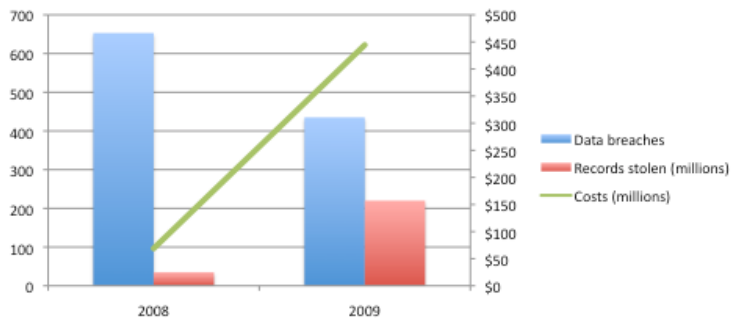


Figure 2 - Cost of a Data Breach (Greenberg, 2009)

Business leaders are more aware of security than ever before, and they understand that the survival of the business depends on keeping information secure (PriceWaterHouseCoopers, 2009); therefore, security leadership roles are gaining the attention of CEO's and Board of Directors.

In PriceWaterHouseCoopers Global State of Information Security 2010 survey, 85% of the respondents reported having either a Chief Information Security Officer or a Chief Security Officer (up from 56%) (PriceWaterHouseCoopers, 2009). The reason for this increased focus in security leadership is due to the increased risk environment and the increasingly tangled web of regulations and industry standards that companies face today (Brenner, 2009).

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

With the increased opportunity for security leadership, comes an increased responsibility for delivery and execution. Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) need to recognize that delivery and execution in 2010 means enhancing regulatory compliance and mitigating risks amidst fast paced change. Enhancing a company's compliance and risk positions amidst fast paced change is a paradigm shift for security. In the past, security was known for processes and tools that either slowed down or even stopped initiatives. Today, security is being asked to formulate strategies and platforms that protect data while allowing it to be used in new and innovative ways. Twitter, Facebook, and Ning are just a few of the growing social technologies that enable viral growth while exposing corporate data to new threats and vulnerabilities (see section **4 References** for growth trends and risks).

As companies invest in new opportunities and technologies, security organizations must evolve their management structure to include a greater focus on data protection, governance, and open collaboration with the business and across the security industry. By focusing on these three areas of management, security organizations, large and small can improve their strategic business importance.

2. Security Management Structures

Businesses' today are in the middle of one of the worst economic downturn in more than thirty years (see inset *Dow: Decade-by-Decade*) and their survival depends on being more competitive and more efficient than ever before. These difficult economic times have also increased risks and threats as hackers focus on greater gains through stealing data as businesses rush to use technologies that may not be fully tested or secure. Unfortunately, current security management structures are ill equipped to handle expanding business requirements while protecting data from unknown risks and vulnerabilities.

Dow: Decade-by-Decade
The Dow has had its second worst decade ever, falling over 8% in the first 10 years of the new millennium. In fact, this decade's performance is only the second time in history that the Dow has fallen over the course of an entire decade, exceeded only by the nearly 40% plunge stocks took back in the 1930s (Hum, 2009)

Organizations today mostly rely on security structures that focus on vulnerability assessment and risk mitigation through technologies and policies that maintain defenses

© 2010 The SANS Institute Author retains full rights.

through asset configuration baselines such as, perimeter firewalls, anti-virus, intrusion detection systems, etc.).

Historically security structures have been dominated by technology; however, Cloud Computing, Software as a Service (SaaS) and Outsourcing are changing the need for technology dominance, replacing it with data protection, governance, and collaboration.

Figure 3 - Security Management Structure

Visually a security management structure can be diagramed as interconnecting disciplines and frameworks (see inset – *Security Management Structure*); where the frameworks contain processes that manage the interactions between the disciplines. Higher performing organizations often deploy security mechanisms and structures as part of a mature IT operational process, such as enterprise security management[2].

2.1. Data Protection Focus

Businesses are searching for new methods and approaches to revenue growth and new means of efficiency and cost cutting, which translates into employees finding new ways of getting more done with less resources. In some instances employees have begun using their own, more capable, productivity systems (i.e. laptops, cell phones, etc), and in other instances they have "benevolently hacked" their way to more productive uses of systems and data (see inset *Hacking Work*).

Hacking Work
(Jensen & Klein, 2010)

The Problem: The tools we use in life have leapfrogged over the ones we use at work. Business's lingering love of bureaucracy, process and legacy technology has fallen completely out of sync with what people need to do their best.

The Breakthrough Idea: Hack work, and embrace the others in your midst who care enough to do so.

The Promise: This kind of work-around isn't new – what is new is that the cheat codes are becoming public and there's nothing you can do about that.

Read the full article at HBR.org

[2] Enterprise Security Management is defined as planning, controlling, & coordinating security activities across an enterprise. Caralli, R. A. (2004). *Managing for Enterprise Security*. Carnegie Mellon University.

© 2010 The SANS Institute Author retains full rights.

The controversy over the use of personal systems is an opportunity for security organizations to reexamine their perspective by focusing on data protection and letting go of asset control. The use of personal systems at work has caught the attention of *CNET*, *Gartner*, *Harvard Business Review* and many others, all contributing their thoughts and opinions to forums and conversations on the web. The views are fairly evenly split between those supporting the practice (as a means of controlling costs) and those opposed to the practice (due to their inability to control the asset).

The argument frames the difference between having a focus on risk management and a focus on data protection. For instance, if a company is focused only on risk management, then physical asset control is certainly a reasonable path to follow; however if a company is focused on data protection then asset control is less of a concern, as virtualization and encryption can offer data protection solutions, and greater flexibility for business users.

> *"The security model is moving to protecting the content not the container, because increasingly the container is not owned by the enterprise. The data is being processed by another enterprise or held in a device used by an individual for their own personal use."*
>
> Dr. Paul Dorey Former Vice President, Digital Security and Chief Information Security Officer, BP; and Director, CSO Confidential (RSA Security Inc, 2009)

Dr. Dorey's comment "data is being processed by another enterprise" introduces the concept of cloud based computing. It is important for a security organization to understand what cloud based computing is and why it is important to the business as they consider the risks it presents.

Cloud based computing, also known as cloud computing or cloud services can be defined as, *"consumer and business products, services and solutions delivered and consumed in real-time over the Internet"*(Gens, 2009). This paper for instance is a cloud based product, stored, secured, and edited using cloud based services (see diagram –

© 2010 The SANS Institute Author retains full rights.

Cloud Services example). By using cloud services I am able to access and edit this paper from multiple places and through multiple devices as long as I have a valid Internet connection.

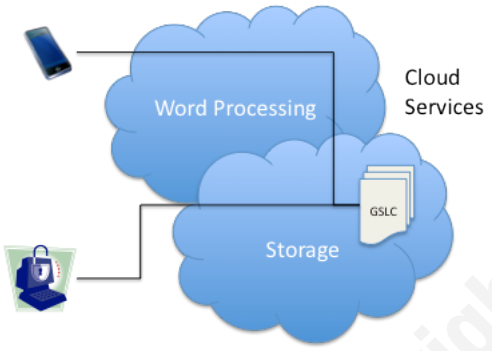


Figure 4 - Cloud Services example

The benefits of cloud services are real and measurable In my example, flexibility and access have been extended from my home to the coffee shop, or wherever I have Internet access through my smartphone[3]. Corporations appreciate these benefits, as lower costs for access help control operational costs during this difficult economic cycle. Workers struggling to stay ahead of layoffs also appreciate these benefits as they use cloud services to communicate and collaborate from any point of connection, which raises their productivity levels[4]. A cloud services model of data creation, use and collaboration, regardless of access methods, highlights the importance of moving to a data protection focus for security management.

2.1.1. A real-world opportunity for Data Protection

One of the most noted data security stories of 2009 is the conviction of Albert Gonzalez, a confessed hacker to several data breaches that set new records for loss. Below is an excerpt of Kim Zetter's article on Albert Gonzales that demonstrates how companies focused solely on perimeter based risk management systems can be exploited.

"Using a SQL-injection attack, two Russian hackers allegedly broke into the 7-Eleven network in August 2007 through the company's website, then routed their way to a server connected to the stores' ATMs, resulting in the theft of an undetermined amount of card data. They allegedly used the same kind of attack to infiltrate Hannaford Brothers in November 2007, resulting in 4.2 million stolen debit and credit card numbers; and into Heartland on Dec. 26, 2007. Of the two unnamed national retailers mentioned in the

[3] While there is no industry standard definition of a smartphone, it is often defined as a mobile phone offering advanced capabilities, such as Internet connectivity & applications
[4] Nonfarm business sector labor productivity increased at an 8.1% annual rate during Q3 of 2009, the largest gain since Q3 of 2003 (U.S. Bureau of Labor Statistics, 2009).

© 2010 The SANS Institute Author retains full rights.

affidavit, one was breached on Oct. 23, 2007, and the other sometime around January 2008.

Once on the networks, the hackers installed back doors to provide them with continued access at later dates. According to authorities, the hackers tested their malware against some 20 different antivirus programs to make sure they wouldn't be detected, and also programmed the malware to erase evidence from the hacked networks to avoid forensic detection." (Zetter, 2009)

The scale of this data breach could have been limited if security, technology and business leaders had simply worked together to understand the threat vectors and vulnerabilities from a data perspective. Had the groups worked together on a data protection focus they could have measured the risk vs. value of having ATM (credit card) data linked to web servers, and could have decided to either separate the data, or take greater precautions, such as encrypting portions of it. Certainly there are still threats to be considered in this example, but they present the point that, a simple change in focus from perimeter defenses to data protection can offer new and flexible solutions that enhance business security, flexibility, and efficiency.

2.1.2. Adopting a Data Protection Focus

Cloud based services are still relatively new and reports on cost savings vary between cloud service vendors and independent agencies, but the promise of lower costs and ease of IT service implementations has corporate leaders willing to fund cloud based service initiatives in 2010 (see *Planned areas of Investment for 2010*).

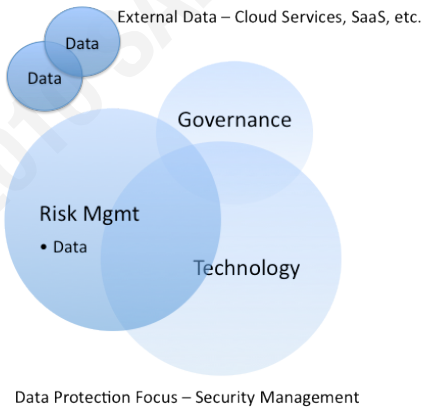


Figure 5 - Data Protection Focus

Adopting a data protection focus begins with understanding that the focus or risk management should include a greater focus on data. Securing the data held in these services begins with the understanding that security and IT no longer have direct control over the location of the data, or how it is accessed; cloud based services and SaaS applications puts users in control of data.

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

Applying the CIA (Confidentiality, Integrity and Availability) rules to data is a good way to frame a data protection focus. Using the diagram – *Data Protection Focus*, consider how to protect the data stored and processed in the cloud based services when you have no means of controlling access to it or who uses it, when 'too risky to allow' isn't an option. One way to resolve this problem is to work with business and technology peers to consider what data should be exposed through a risk vs. value governance process that balances corporate growth and efficiency with regulatory compliance.

What is evident is that protecting data is no longer a pure technology task; a data protection focus relies on governance and open business collaboration.

2.2. Governance

With greater importance being placed on the security and compliance of organizational data, security leaders need to include corporate governance[5] as a part of their management structure. It is important to understand that governance in this instance is not a set of policies; rather governance is the structure used to approve the policies and methods of monitoring that *meet business needs*. Meeting business needs is critical to governance, if policies and measurements add more control, oversight and cost than a business needs, then governance will not be followed. Conversely, if policies and measurements fail to ensure regulatory compliance, then governance is not protecting the business.

Governance Resources

CERT - Governing for Enterprise Security

ISICA - Implementing and Continually Improving IT Governance

IT Governance Institute - Board Briefing on IT Governance, 2nd Ed

ISF - Standard of Good Practice

International guides ISO/IEC 27002 and COBIT

Links active at time of writing.

Governance is needed in both large and small organizations and can be implemented in various forms and sizes with the help of industry references and resources (see inset *Governance Resources*). The best governance structures involve business leaders and their objectives. In 2010, that means supporting initiatives such as centralization, social knowledge and cloud computing. Security leaders must work with their peers to accelerate the adoption

[5] In this paper, governance is defined as the structure through which the objectives of the enterprise are set, and the means of attaining and monitoring them are determined

© 2010 The SANS Institute Author retains full rights.

of these technologies ensuring they increase efficiencies and reduce costs while protecting organizational data and reducing risk. Unfortunately, not all risks will be understood during the development and implementation of these initiatives, which makes it even more important to evaluate and articulate the risks as part of a balanced governance system.

Putting governance in place is difficult; making sure it is effective is even more challenging. Consequently, it is important to understand the goals of governance and what makes the structure effective before attempting to implement one. Unfortunately, the term governance usually brings up visions of bureaucracy, committees, and endless meetings, rather than the goals of *Transparency*, *Shared Ownership*, *Feedback*, and *Linkages to business goals and Objectives*.

How an organization goes about achieving governance is in large part a reflection of its organizational culture and structure. Security personnel need to understand the organization they are in when designing and implementing governance, as each organization is unique and no single approach will work for every situation.

2.2.1. A real-world failure to adequately measure threats and vulnerabilities

The TSA is one of the most visible and well-funded security organizations in the United States, yet its recent failure to fully assess the threats and vulnerabilities the transportation system faces has limited its effectiveness. In a recent news story released by the Associated Press, the Government Accountability Office testifying before Congress made the following statement regarding the efficiency and effectiveness of the Transportation Security Agency (TSA):

"…The TSA has not completed this full assessment of threat, vulnerability and consequences together. As a result, TSA cannot get a complete picture of the potential risk from any particular threat and it cannot be sure that its investments in screening devices address the greatest risks to aviation" (The Associated Press, 2009).

> *"security breaches are ultimately caused by a failure in a process or implementation of a security policy"*
>
> Cem Paya, a data security expert at Google (Knowledge@Wharton, 2009)

© 2010 The SANS Institute Author retains full rights.

2.2.2. Moving Forward with Governance

Failing to fully understand risk is a breakdown in governance. In the TSA example, a continual analysis and feedback system focused on risks could have alerted the TSA to the new and growing threat facing passengers. Successful security structures include governance and large and small security organizations must proactively pursue a comprehensive governance process that fits business needs and corporate culture.

Figure 6 - Governance

The importance of a business-aligned, feedback-based governance system cannot be understated; without the balance these elements offer, technology may become the single focus for protecting the organization (see diagram – *Governance*). Consider if you will the implication of a security focused perimeter defense strategy, an overwhelming urge to protect all data at the endpoint could lead to high system loads and drive users to 'benevolently hack' (see inset – *Hacking Work*) their way around under-performing systems to accomplish their goals. Despite its importance, many organizations do not have a governance system in place, or they fail to measure the effectiveness of the governance process. Consider these questions to help you measure governance effectiveness in your organization:

Do you know where your data is? In the PriceWaterHouseCoopers survey, six out of ten respondents (60%) reported that their organization did not have an accurate inventory of locations or jurisdictions where personal data for employees and customers was collected, transmitted, and stored. (PriceWaterHouseCoopers, 2009) Working with business and technology peers and leaders, risks to data can be analyzed and mitigated.

Are you examining new business technologies? In 2009, only four out of every ten respondents (40%) in the PriceWaterHouseCoopers survey reported that their organization had security technologies that supported Web 2.0 exchanges, such as social networks, blogs, and wikis (PriceWaterHouseCoopers, 2009). Partnering with business

© 2010 The SANS Institute Author retains full rights.

and technology leaders (those responsible for procuring business technology) security organizations can take a pro-active approach to risk analysis and mitigation.

Do you have an annual plan that lists business initiatives with supporting security initiatives and technologies? This question is often one of the most difficult to answer, as security planning is still relatively new. Security, mostly seen as a technology province, has often been left out of planning discussions. Security leaders must take a more active interest in collaboration, seeking to understand business and technology plans in order to design and deploy, efficient security systems and measures that work with new technologies, products, and services.

Andrea Matwyshyn, author of *Harboring Data: Information Security, Law, and the Corporation* perhaps summarized the need for governance in a recent interview with Knowledge@Wharton

"There's a broader lack of planning in many enterprises. In their defense, this field is relatively new. However, the downside of not securing information assets is so severe that it's important that companies start to focus on process-based, top-down initiatives to incorporate information security at every level of their enterprise. Really the neglect is reaching the point that ... an argument could be made that the lack of planning that's prevalent in U.S. companies may give rise to cause a breach of fiduciary duty. That's serious. We've reached a turning point. This is when it really needs to be addressed aggressively in a process-based approach throughout enterprises."
(Knowledge@Wharton, 2009)

2.3. Open Business and Industry Collaboration

Open business and industry collaboration may not seem like valuable part of a security management structure, until you consider that an effective security program requires an understanding of present and future business plans along with the security risks they present and the ability to constructively mitigate those risks with peers, colleagues and mangers.

Governance and data protection mechanisms are good initiators of business collaboration, but they are not enough to demonstrate that security can be a strategic part

© 2010 The SANS Institute Author retains full rights.

of the business; only through business knowledge and industry collaboration can security change from being a reactive organization to proactive strategic business function.

To help demonstrate value in industry and business collaboration, consider how insights provided in Verizon's Data Breach (Verizon, 2009) analysis can help security organizations outline initiatives to protect business data and record loss.

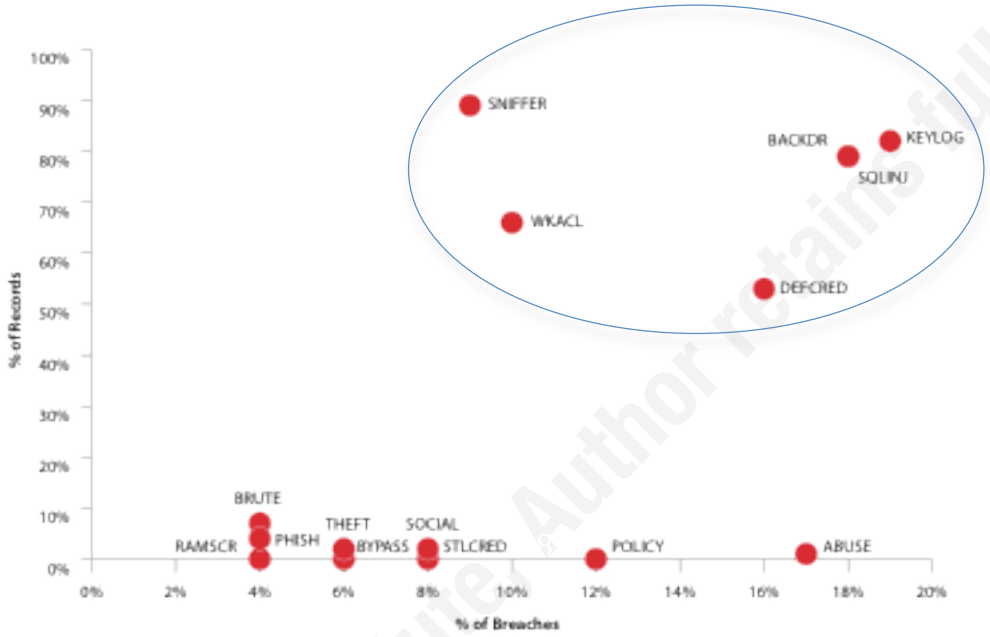


Figure 7 - Records lost by Breach vector (Verizon, 2009)

Verizon determined that one of the common causes behind the six highest vectors of data loss (circled in the diagram – *Records lost by Breach vector*) was inappropriate applications installations, most often allowed through misconfigured privileges or by errant user behavior. By sharing this information security teams can focus on preventative measures. This example helps demonstrate that shared knowledge unrestrained by competitive fears, can benefit businesses.

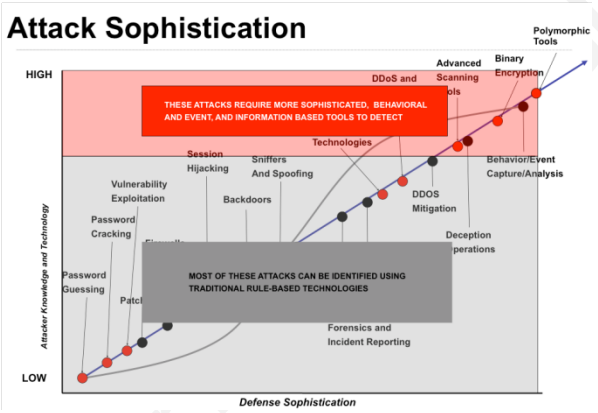
2.3.1. Understanding and Meeting Demands

The Internet has expanded growth and wealth for business and individuals. Consequently the inter-connectivity of business, systems and individual has also increased both the business and technical risks they face – for instance, losses from

© 2010 The SANS Institute Author retains full rights.

global inter-linked loans and mortgages affected businesses across the globe, while growing networks of inter-connected systems multiplied cyber-theft threat vectors.

To counter earlier threats, security organizations deployed systems of perimeter defenses (proxy systems, firewalls, anti-spam systems, etc.), and restrictions to curtail unsafe user activity; today however attacks are more sophisticated, employing multiple threat vectors and distributed command and control systems to maximize effectiveness while avoiding detection. CERT located at Carnegie Mellon University's Software Engineering Institute plotted how attack sophistication has outpaced defenses, see the inset – *Attack Sophistication*) (CERT, 2009).



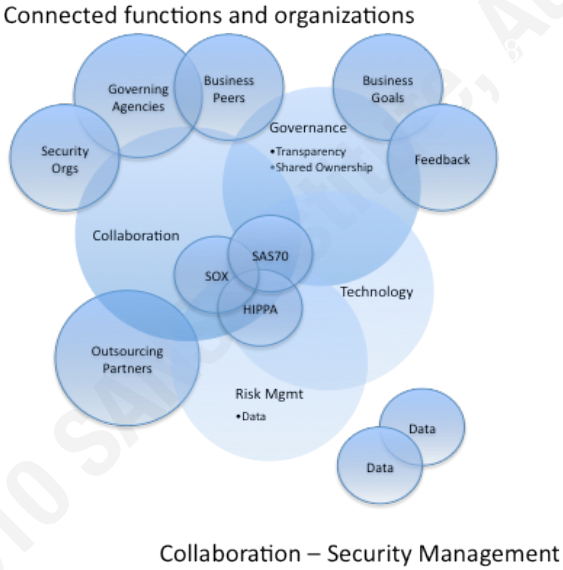


Figure 8 - Collaboration

The value of threat and risk intelligence is at a premium; open business and industry collaboration is essential for developing the insights needed as businesses continue to link together networks for growth and efficiencies. Collaboration must expand with technologies, services, and requirements as shown in the diagram – *Collaboration*.

Another reason for increasing collaboration is in addressing the top-down concerns of corporate executives. In the PriceWaterHouseCoopers Global State of Information Security 2010 survey, seventy-six percent (76%) of the respondents reported that the increased risk environment

© 2010 The SANS Institute Author retains full rights.

had elevated the importance of cyber security among the top executives, while 77% said the increasingly tangled web of regulations and industry standards has added to the sense of urgency. Additionally, the harsher economic realities raised data protection concerns among 70% of the respondents while 68% cited the need to strengthen the company's governance, risk, and compliance programs (PriceWaterHouseCoopers, 2009).

Clearly, executives have top down concerns that security organizations must address through collaboration with technology and business peers and leaders. This has often been a challenge for security that even today remains a subject of debate as many security professionals favor organizational and reporting independence, rather than collaboration as a means of governance. The position I present in this paper is that collaboration with business and technology peers is essential to securing data and ensuring compliance with regulatory guidelines. Notably, there are instances where defined authority is necessary for regulatory compliance, but these instances neither hinder nor impede collaboration.

Outsourcing is an additional point of collaboration for security organizations. Again, this topic is controversial, but a healthy governance model will examine the various forms, costs, benefits and risks of in-house and outsourced security. For instance, many organizations today find that outsourcing anti-virus scanning and email services is more cost effective than maintaining it in house – this form of outsourcing allows security staff to focus on more critical aspects of the business' security.

Fortunately, there are external resources and communities' security organizations can turn to for help and information exchange, such as:

The Information Sharing and Analysis Centers – set up to establish and maintain a structure for interaction on cyber and physical security issues between and among private and public sector organizations in North America.

The CERT Coordination Center (CERT/CC) – addressing risks at the software and system level. Established as an incident response team, the CERT/CC has evolved, focusing on identifying and addressing existing and potential threats, notifying system administrators and other technical personnel of these threats. CERT coordinates with vendors and incident response teams worldwide.

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

IT Security Essential Body of Knowledge (EBK) – competency and functional structure for IT security workforce development that conceptualizes security skill requirements in a new way to address evolving IT security challenges.

National Vulnerability Database (NVD) – U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). The NVD enables the automation of vulnerability management, security measurement, and compliance through databases of security checklists, security related software flaws, mis-configurations, product names, and impact metrics.

3. Conclusion

Economic and political conditions have changed the operating environments for businesses. Today businesses are forced to adopt new technologies that grow revenues and attract new customers; while illegal demands for their intellectual property and customer data continues to grow. These challenges have created a greater need for, and placed more importance on security as a function of business strategy; security today is no longer just a technology province.

Recognizing the need for security to become a part of business strategy, CEOs and Boards of Directors have invested in security leadership and technologies. In PriceWaterHouseCoopers Global State of Information Security 2010 survey, 85% of the respondents reported having either a Chief Information Security Officer or a Chief Security Officer, a 29% increase in leadership in a single year (PriceWaterHouseCoopers, 2009).

This new downward driven focus on security is an opportunity for security organizations and leaders to re-examine their fundamental view of security; in 2010 and beyond, security organizations need to balance risk and value to enable innovation. This is a paradigm shift for security organizations, as they now must develop the focus, tools, and relationships necessary to define and assess the level of acceptable risk for each new business innovation.

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

Understanding and approaching these changes can be a difficult transition for security leaders and personnel; business goals and objectives must frame security decisions, governance will measure compliance, data protection will guide technical decisions and collaboration will drive enhancements. This paper introduced these concepts as additions and extensions of existing security structures that can be applied by both large and small organizations.

Challenges will continue to dominate business' future as economic and political threats raise the demand for stolen intellectual property and data while new methods designed to increase productivity present new vulnerabilities which criminals exploit with escalating sophistication and speed. By adopting a strategic, data focused, governance driven and collaborative approach to information security management, security organizations will be equipped to deal with the constant evolution of technology and escalating pace of change. If we achieve this goal, our businesses will reap the rewards of globalization and technology even in the face of unprecedented risk and severe economic conditions.

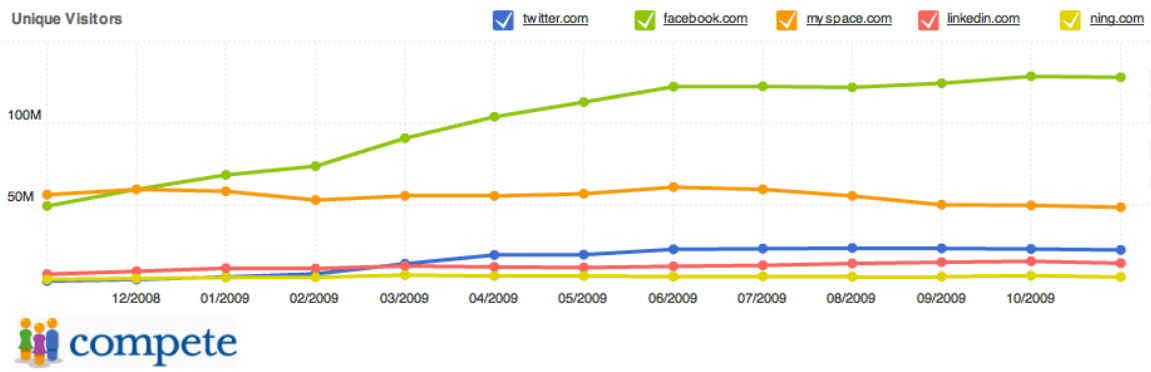
> *"The enterprise is drastically changing, not just who we connect to or how we connect to them or who has access to what information, but the basic premise that our enterprise or corporate operating environment is now migrating outside of our basic operational control infrastructure."*
>
> Roland Cloutier Vice President, Chief Security Officer EMC Corporation (RSA Security Inc, 2009)

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

4. References

4.1.1. **Social Knowledge growth rate in 2009** (unique visits per month)



4.1.2. **Sample of Social Knowledge risks** (links active at time of writing)

Top 10 security and privacy stories concerning Facebook & Twitter (Brodkin, 2010)

Risk: Hijacking Accounts
Jan. 6: Hackers hijack Obama's, Britney's Twitter accounts

Risk: Worms & Viruses that use the social media platforms to spread
April 11: Twitter wrestles with multiple worm attacks

Risk: Phishing (common and spear-phishing) attacks
May 18: Phishers, viruses target Facebook users

Risk: Hacked Cloud Apps
July 15: Twitter/Google Apps hack raises questions about cloud security

Risk: Denial of Service attacks
Aug. 6: Twitter victimized by distributed denial-of-service attack

Risk: Botnet attacks
Aug. 14: Twitter used to manage botnet

Risk: Spammer attacks
Oct. 30: Facebook awarded $711 million in spammer case

Risk: Legal challenges
Dec. 8: Facebook shuts down Beacon program, donates $9.5 million to settle lawsuit

Risk: Controversy
Dec. 9: Facebook unveils controversial new privacy settings

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

5. Bibliography

Brenner, B. (2009). *Why Security Matters Again.* CIO Magazine.
Brodkin, J. (2010 йил 7-Jan). *Social networking hacks: Top 10 Facebook and Twitter security stories of 2009*. Retrieved 2010 йил 8-Jan from Networkworld.com: http://www.networkworld.com/news/2010/010710-social-networking-hacks.html?page=1
Caralli, R. A. (2004). *Managing for Enterprise Security.* Carnegie Mellon University.
CERT. (2009 йил 2-Oct). *The Physics of Information Security.* Retrieved 2010 йил 6-Jan from Infragaurd - Pittsburg: http://www.infragard-pittsburgh.org/events/2009/psc-cert.pdf
Complete Inc. (2010 йил 7-Jan). *Siteanalytics*. Retrieved 2010 йил 7-Jan from Complete.com: http://siteanalytics.compete.com/twitter.com+facebook.com+myspace.com+linkedin.com+ning.com/?metric=uv&months=12
Gartner Inc. (2008). *Assessing the Security Risks of Cloud Computing.* Gartner Inc.
Gens, F. (2009). *Clouds and Beyond: Positioning for the Next 20 Years in Enterprise IT.* IDC.
Greenberg, A. (2009 йил 24-Nov). *The Year Of The Mega Data Breach*. Retrieved 2009 йил 12-Dec from Forbes.com: http://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches_print.html
Greengard, S. (2009 йил Dec). 10 Trends for 2010 Piecing Together a Strategy. *Baseline* (101), pp. 16-22.
Hum, R. (2009 йил 29-Dec). *Dow: Decade by Decade*. Retrieved 2009 йил 29-Dec from CNBC: http://www.cnbc.com/id/34619797/site/14081545
Identity Theft Resource Center. (2009 йил 29-Dec). *Data Breaches.* Retrieved 2010 йил 6-Jan from Idtheftcenter.org: http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#
Jensen, B., & Klein, J. (2010 йил 1-Jan-Feb). Hacking Work, Learn to love the rule breakers. *Harvard Business Review , 88* (1), pp. 53-54.
Knowledge@Wharton. (2009 йил Aug). Information Security: Why Cybercriminals Are Smiling. *Knowledge@Wharton* , 6.
Mills, E. (2009 йил 1-Feb). *Data breaches cost $6.6 million on average, survey finds*. Retrieved 2009 йил 12-Dec from CNET: http://news.cnet.com/8301-1009_3-10153858-83.html
National Institute of Standards and Technology. (2008). *NIST Special Publication 800-55 Revision 1.* Gaithersburg: National Institute of Standards and Technology.
PriceWaterHouseCoopers. (2009). *The Global State of Information Security Survey, 2010.* PriceWaterHouseCoopers.
RSA Security Inc. (2009). *Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk.* RSA Security Inc.
The Associated Press. (2009 йил 29-Oct). Audit: Airport screening needs more risk study.
The SANS Institute. (2009). *Managment 512 SANS Security Leadership Essentials.* The SANS Institute.

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.

U.S. Bureau of Labor Statistics. (2009 йил 3-Dec). *Productivity and Costs, Third Quarter 2009, Revised.* Retrieved 2009 йил 3-Dec from www.bls.gov: http://www.bls.gov/news.release/prod2.nr0.htm
Verizon. (2009). *2009 Data Breach Investigations Supplemental Report.* Verizon.
Zetter, K. (2009 йил 21-Dec). *Albert Gonzalez Enters Plea Agreement in Heartland, Hannaford Cases*. Retrieved 2009 йил 26-Dec from Wired.com: http://www.wired.com/threatlevel/2009/12/gonzalez-guilty-plea-heartland/

© 2010 SANS Institute, Author retains full rights.

Dale Emel, dale.emel@gmail.com

© 2010 The SANS Institute Author retains full rights.