Journal of Information Technology Education: Discussion Cases

9/05/2016

ERIC BIEL, NORMA GONEDES, DARIN PEACHEE, EDGAR RAMIREZ, JING YANG, BRIAN MURPHY

# THE QUEST FOR RELIABLE CYBER SECURITY[1]

> *"There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."*
> *- FBI Director James Comey*

The sun set on another long day at the headquarters of *ReliaQuest* where Brian Murphy leaned back in his chair and exhaled deeply as he considered the cyber security breaches that had consumed the media in recent weeks. Retail giants like Target, Lowe's and Home Depot had fallen victim to serious data breaches. He pondered how his company, *ReliaQuest*, could make a difference in a world saturated with an invisible army of hackers. Companies had to fend off attacks 100% of the time, but the hackers only had to be successful once.

As Brian contemplated the brand new Secure Operations Center (SOC) being built in his offices in downtown Tampa, he reflected on his recent pitch to a multi-billion dollar global medical device company. The company wanted all of *ReliaQuest's* solutions—the Assess, Secure, and Manage options. This would be a multi-million dollar contract over several years. But the CIO and CEO had been very clear, with the contract would come a demand for a 100% guarantee that *ReliaQuest* solutions would prevent any information system breach and eliminate the possibility of any loss of data for their customers, suppliers, or employees.

Cyber security, as Brian thought of it, was the largest and most expensive cat and mouse game in the corporate world, and often undervalued by companies until a breach occurred. How could *ReliaQuest* offer solutions that companies would value with or without a breach? How could Brian's team provide alternatives to companies who frequently did not even understand the wide variety of cyber security threats? What kinds of risks to data and information security were acceptable? What was the cost/benefit analysis on a breach? What sort of role should the client company play in protecting their data and that of their customers, vendors, and employees? Was there such a thing as too much security? Certainly there could be too little security, right? Could *ReliaQuest*, or any cyber security company, "guarantee" zero breaches, or losses of sensitive data and information? What could *ReliaQuest* offer its clients when every solution promised came with the risk of a breach and loss of data?

---

# Cyber Security

Brian began his career at *PricewaterhouseCoopers LLP* where he was a management consultant. Although he enjoyed the consulting, his entrepreneurial spirit drove him to break away from the corporate world and start his own company. The concept for *ReliaQuest* was sketched out on some cocktail napkins by friends having a few drinks at an alumni event at *Florida State University* (FSU). Brian was at the center of this group of FSU alumni. Shortly after returning home, he incorporated, and the start-up began operating in late 2007 with three phones and two employees.

Since its inception in 2007, *ReliaQuest* had become one of the fastest growing and cutting edge information technology security consulting firms in the United States. The majority of *ReliaQuest's* early business came from operating as a subcontractor to large prime contractors providing engineering services to the United States Military. *ReliaQuest* provided resources all over the world in information assurance (later known as cyber security), network engineering, and satellite engineering. As the overseas environment became more and more hostile, Brian began to focus on commercial markets in the US. The need for a commercial solution for cyber security attacks was growing rapidly in scale and visibility. The company's commercial practice grew rapidly. With growth came a decision to shift the focus to commercial activity that quickly came to represent more than 90% of its revenue.

Brian felt he understood the ever evolving nature of the cyber security realm. Companies in the business world faced off with an almost infinitely large, unknown force that threatened the security of their data on an everyday basis. Even when a company would recognize that there was an attack, frequently there was little that could be done with their internal IT resources to combat it, or prevent a different type of attack from happening again. Brian was determined to build the *ReliaQuest* team of engineers into a preferred solution to this problem. As he adapted his security solutions business to this need, Brian found that his focus was on getting prospective companies to take data and information security from an afterthought cost of doing business to an essential asset to the business that provided value customers would pay for knowing that the products and services provided were secure.

Brian felt good about what *ReliaQuest* had to offer, but as companies came knocking at the door asking for their services, he and his team had to work hard to help companies understand the importance and nature of this elusive thing called "cyber security". It was one thing to buy a bunch of software positioned to solve all of an organization's problems, but it was another to make all that technology work together efficiently and effectively. How could he educate potential clients about information security and why it really mattered?

## Why Did Information Security Matter?

Firms collected, stored, managed and transferred information on a daily basis to either provide services or to produce goods for customers. That information was considered an asset of the firm because it added value to the business. Like any asset of the firm, data and information should be properly secured and protected. As business has come to rely heavily on the digitization of every type of data important to the operation of the business, the pace of data accumulation and the number of systems that collected, stored, managed and transferred data increased exponentially. Today, every business has become an information systems reliant business.

The growing dependence on information systems, shared networks and distributed services like cloud computing had one significant drawback. Every system, every collection and reporting technology, and every data storage and transmission device was vulnerable to cyber security attacks. And there were multiple types of attacks possible at every point of system access.

## Cyber-Attacks

Brian and his team knew that cyber-attacks were increasingly sophisticated, and often executed in highly intelligent, staged and persistent ways by professional criminals. The 2014 "Data Investigations Report" defined an incident as a security event that compromises the integrity, confidentiality, or availability of an information asset. A breach was defined as an incident that resulted in the disclosure or potential exposure of data. A data disclosure was a breach for which it was confirmed that data was actually disclosed, and not just exposed to an unauthorized party (*Verizon Data Breach,* 2014).

"The FireEye" cyber security report (Exhibit 6) identified five stages in a typical advanced type of attack.

1. *External Reconnaissance:* Attackers searched for potential targets to identify "persons of interest" or "points of access" and assess their weaknesses.
2. *Initial Compromise:* Attackers used "phishing" emails, spam messages or watering-hole attacks to "spear" weak actors, and gain access to the system.
3. *Foothold Establishment:* Attackers tried to get administrative credentials, and to install stealthy "malware" in the victim's system to avoid detection of host-based or network-based security measures.
4. *Internal Reconnaissance:* Attackers gathered information on surrounding infrastructure, trusted relationships and operating system domain information to locate the valuable assets, and transfer them out of the system. Attackers also frequently prepared for re-access if detected by deploying additional backdoors into the system.
5. *Mission Completed:* Packaged and stole target data. After stealing data, attackers would try to retain access for future attacks by covering their tracks to avoid detection.

The vulnerability of any company's network had gone far beyond hacking through a firewall. Now attacks focused on the vulnerability of the entire organization with access provided through embedded devices, vendor connection points, and clever co-opting of employee usernames and passwords. These more sophisticated attacks could occur with no one knowing the breach had occurred, or that data was missing (Savoie, 2012). But Brian's team had discovered that most businesses were not even aware of the incidents or breaches that had, or were currently occurring to their systems.

### *Threats to IT Systems and Information*

The *ReliaQuest* team knew that threats to information systems and data came in many forms and included:

- *Hardware and software failure* - such as power loss or data corruption.
- *Malware* - malicious software designed to disrupt computer operation.
- *Viruses* - computer code that could copy itself and spread from one computer to another, often disrupting computer operations
- *Spam, scams and phishing* - unsolicited email that sought to fool people into revealing personal details or buying fraudulent goods.
- *Human error* - incorrect data processing, careless data disposal, or accidental opening of infected email attachments (IT Sector Coordinating Council, n.d.).
- *Hackers* - people who illegally broke into computer systems.
- *Fraud* - using a computer to alter data for illegal benefit.
- *Passwords theft* - often a target for malicious hackers.
- *Denial-of-service* - online attacks that prevented website access for authorized users.
- *Security breaches* - included physical break-ins as well as online intrusion.

- *Staff dishonesty* - theft of data or sensitive information, such as customer details (IT Sector Coordinating Council, n.d.).
- *Backdoors* – generally code that exploited a weakness in the system administration.
- *Exploits* – software that took advantage of a known or discovered system bug or glitch.

The number of attacks and breaches differed by type of actor and actor motivation, and had grown dramatically over the prior ten years (a partial list is presented in Exhibits 11 and 12). Moreover, the time for an attack to lead to a compromise was falling even as the time to detect a breach was rising (Exhibit 13). *ReliaQuest* was especially concerned with identifying the appropriate defense for every possible attack.

## Cyber Defense Types: Passive and Active

Cyber defense approaches were generally classified as passive or active (Security Architecture for Open System Interconnections Standards - ISO 270k). Passive defense focused on monitoring all network activity with the goal of collecting information to identify attackers. Passive defense approaches surveyed message content and performed traffic analysis. Active cyber defense often involved the identification of attackers through the "baiting" of potential bad actors with a false data stream or data repository. Baiting might take the form of "masquerade, replay, modification of messages, and denial of service" (Stallings, 2013). Sometimes the team found that a mock server set up as a "honey pot" could attract the bad actor "cyber flies," and they could observe and learn from the resulting attacks.

## The Cyber Defense Challenge: Prevention vs. Detection

*ReliaQuest* customers frequently identified that for them the purpose of information security management was to ensure business continuity, prevent information related problems (security incidents, and minimize the impact of these incidents when they occurred) (Exhibit 1). *ReliaQuest* knew that, ultimately, any cyber security effort must ensure three basic dimensions of information security: Confidentiality, Integrity and Availability (CIA). These three dimensions are better remembered as the CIA triad (Agrawal, Campoe, & Pierce, 2014). They defined each as:

- *Confidentiality* referred to limiting information access and disclosure to authorized users--"the right people"--and preventing access by or disclosure to unauthorized ones--"the wrong people."
- *Integrity* referred to the preservation without corruption of whatever was transmitted or entered into the system, right or wrong. Integrity also referred to the trustworthiness of information resources.
- *Availability* referred to the availability of information resources.

The *ReliaQuest* team recognized that securing information was a tradeoff between these three dimensions. They knew that when it came to information security, companies differed widely in their emphasis across the dimensions. Some companies sought to block all suspect access, and were willing to sacrifice availability of the data or the system for security. Other companies were committed to open access to information by the widest possible set of users to optimize operational efficiency. Still others, focused almost exclusively on systems that maintained data integrity and insured its utility to users.

Thus, information security was a combination of prevention and detection across the dimensions of confidentiality, integrity and availability. Brian believed that the balance between prevention and detection depended heavily on the client company and the available security technologies. While the relative risks associated with these categories depended on the particular context, frequently humans were the weakest link. Poor supervision of staff and lack of proper procedures when it came to security were often the major causes of security incidents (Exhibit 2).

Ultimately, cyber security as a service (CSaS) required companies like *ReliaQuest* to understand how the customer might balance passive and active defenses with the need to prevent and detect attacks. Realistically, companies were beginning to realize that they could not do it alone. In fact, partnering with third party vendors (like *ReliaQuest*) was becoming essential to the balance (Zolper, 2014). Brian also knew that no single cyber security company could know all the threats, or develop all possible solutions in this fast growing and quickly changing industry. In the cyber security industry, Brian intuitively understood what was found by the Global State of Information Security® Survey 2014--82% of companies that possessed high-performing security practices were collaborating with others to deepen their knowledge of security solutions and evolving threats (*The Global State of Information Security® Survey,* 2014).

# Cyber Security Industry

*"The Cyber Security industry is made up of companies that provide security products and services for offensive and defensive applications across the internet, internet connected devices, telecommunications equipment and industrial domains"* (*PWC Cyber Security M&A Report,* 2011).

## Market Size and Projected Growth

Research from Gartner predicted that cyber security spending would outpace the U.S. GDP and mobile device growth, and increase 7.9% to $71.1 billion in 2014. Projections indicated that it would grow another 8.2% to reach a market size of $76.9 billion in 2015 ("Global Security Spending," 2014).

Brian knew that the main drivers of the industry were:

- Increased cyber threats from more sophisticated cybercrime groups.
- Increased security awareness from companies and consumers.
- Greater systems vulnerabilities due to the inter-connectivity of networks.
- Greater accessibility of users through mobile devices and virtual "cloud" services.
- Growth in technology driven products and services (including the internet of things).
- Tougher data security regulations and industry compliance requirements.
- Growth in social networking, e-commerce and e-banking.

Brain also knew that the bring-your-own-device (BYOD) to work trend was making life more difficult as device endpoints went from static (desktop, servers, routers) to mobile with significant demands on device interconnectivity and downloadable software applications (Fraiha, n.d.).

## Market Sectors and Emerging Trends

In most countries, the major consumers of cyber security products and services were split between the public and the private sectors. The U.S. federal government, alone, spent an amount almost equal to that of the private sector. In the private sector there were small, medium and large companies that varied in cyber security spending patterns and outsourcing strategies (Exhibit 3).

Larger companies with revenue of more than $1 billion tended to invest heavily in more mature security processes and technologies in order to enhance their existing security infrastructure, and frequently maintained security centers of their own. Medium-sized companies with revenue ranging from $100 million to $1 billion tended to be less able to afford a sophisticated internally operated cyber security center. These companies were turning more and more to managed cyber security service providers for CSaS as the threat actors were increasingly stepping up their assaults on middle-sized companies. Small companies with revenue under $100 million that once considered themselves unattractive to hackers were starting to pay more attention to security services as their customers, who were often large sized companies, were

putting stricter IT security thresholds upon their commercial partners and supply chain vendors (*PWC. Managing Cyber Risks Survey,* 2015).

Interestingly, even as total expenditures on cyber security were growing (Exhibit 3), companies were finding a need to be very judicious in their spending. As Exhibit 4 shows, large company spending on IT overall and the percentage spent on security solutions was relatively flat in the prior two years. Security experts suggested this was primarily due to a need for companies to allocate security budgets more effectively to focus on their most valuable data, rather than attempt to protect all data. Brian found that the largest companies needed to "do more for less" with spending on cyber security measures competing for scarce IT resources with enterprise IT investments, IT systems maintenance budgets, IT infrastructure investments, and IT spending on decision support and data analytics and management. Frequently, *ReliaQuest* found that the more customer, revenue, and cost management focused IT systems "won" the budget battle at the expense of the cyber security spending.

When companies did spend on cyber security, according to the PwC 2015 Global Survey, the top five overall spending priorities for companies were: employee security awareness training, user account management, user behavior profiling and monitoring, smartphone encryption, and tools for data loss-prevention. Several prominent and growing needs in cyber security were mobile security strategy (MSS), mobile device management (MDM), and mobile application management (MAM)--solutions which had increased from 39% to 47% in terms of importance in just the last year (Exhibit 5) (*PWC. Managing Cyber Risks Survey,* 2015).

Brian knew the industry was booming, and the need was growing for companies at every level. And he saw that the number and types of solutions and cyber security providers were growing rapidly too. As Brian considered the threat and solution landscape, he knew he needed to find the solution set that would make sense for *ReliaQuest* to offer.

## Emerging Cyber Security Solutions

Consumers (and many company executives) tended to be familiar with relatively simple firewall or threat-signature based security software solutions like Norton and McAfee, and thought of cyber security only in those terms. They were also often experienced with various appliances that could lockout hardware or software. All enterprise employees were familiar, at some level, with passwords, user-ids, and security training. Unfortunately, the cyber security solutions landscape for enterprises was much more complex than that.

According to the 2014 "Cyber Security - Emerging Trends and Investment Outlook," there were 191 major cyber security companies operating in the cyber security market and thousands of smaller players. As shown in Exhibit 5, the NIST Cyber security framework identified solutions as either "Detect" or "Respond" and ran the gamut from compliance management to disaster recovery and everything in between. Typically, cyber security solution providers offered one or more solutions in one or more of the cyber security functional areas–identification (ID), protection (PR), detection (DE), response (RS), and recovery (RC). The framework was a U.S. government-industry collaboration to categorize all of the areas governmental agencies and companies needed to consider for improving their cyber security posture. Each functional area was broken down into several categories for a total of 22 categories requiring companies' attention. The categories were further divided into subcategories referenced by various governmental and industry standards or guidelines ("Framework for Cybersecurity," 2014).

Many cyber security system providers took a security information and event management (SIEM) approach to provide a more integrated, non-signature-based, real-time, adaptive security solution. In his mind, SIEM approaches were essential to target and defeat the highly intelligent new generation of cyber-

attacks that unfolded in stages, exploited systems across multiple threat vectors (different OS systems, different device platforms), and were stealthy and custom-tailored to the target company. SIEM software products and services combined security information management (SIM) and security event management (SEM). SIEM solutions provided real-time analysis of security alerts generated by network hardware, software and appliances; managed services that logged sensitive data access; and provided sophisticated reporting for decision support ("Framework for Cybersecurity," 2014). The major cyber security industry players that offered full-fledged SIEM solutions included: HP ArSight, IBM Security, QRadar, SPLUNK, Log Rhythm, and McAfee ESM ("SIEM: A Market Snapshot," 2007).

## Competitive Landscape

In 2013, the four largest companies in the cyber security provider industry accounted for only an estimated 13% of industry revenue. The services provided by the larger companies varied to include technology consulting, management consulting, and financial consulting in addition to SIEM. Even with the handful of large global cyber security focused corporations, the cyber security provider industry was exceedingly splintered (Hkrabeepetcharat, 2013).

There were a significant number of independent contractors, and small-scale, specialized companies in the cyber security field. The industry had experienced a level of consolidation from acquisition and merger activities over the past five years. Frequently, consolidation occurred as larger companies in the industry acquired smaller cyber security firms with a competitive advantage in a niche market (such as a password encryption or identity theft capability).

As Brian considered the competitive landscape, he felt that *ReliaQuest* had a few major competitors in addition to many smaller players. Two players that typified the range of his primary competition for his clients were *Accenture* and *FishNet Security*.

*Accenture Ltd* typified the all-in-one services provider and included management consulting, outsourcing, security, and many other services with more than 305,000 employees, offices and operations in more than 200 cities in 56 countries, and net revenues of $30.0 billion for fiscal 2014. *Accenture* was focused on four growth platforms—Accenture Strategy, Accenture Digital, Accenture Technology, and Accenture Operations. They touted the four as the innovation engines through which they built and offered world-class skills and capabilities, developed knowledge capital, and created, acquired and managed key assets central to the development of integrated services and solutions for their clients (https://www.accenture.com/us-en/company.aspx).

*FishNet Security*, on the other hand, was a more recent, nimble provider of information security solutions. They focused on security solutions that combined technology, services, support and training. "Since 1996, the company has enabled clients to manage risk, meet compliance requirements and reduce costs while maximizing security effectiveness and operational efficiency." *FishNet Security* claimed it had delivered quality solutions to over 5,000 clients worldwide (https://www.fishnetsecurity.com/company).

Brian realized that he needed to develop a targeted set of solutions for firms across the size and security sophistication spectrum, where he wanted to focus *ReliaQuest* efforts, if he were to compete effectively with his young company. He believed he had the team, the talent, and the technology to make it happen.

# ReliaQuest

## Customers

*ReliaQuest*, since moving to commercial business, worked with customers that ranged from regional healthcare and financial institutions to the Fortune 50 companies. Their goal was to help customers truly understand the threats they faced, and then help them to implement and optimize their security platforms to stay ahead of the threats.

Brian wanted clients to know that security was not a losing battle, despite what many "experts" had said in the wake of the Target, Lowe's and Home Depot attacks. He advocated that it was not as simple as spending a lot of money, and then being able to safely say that the company was secured. He shared with every customer that the road toward improved information security required a persistent, surgical application of technologies and procedures that needed to become a way of doing business for the client company.

As the team started the year, they brainstormed where they had come from and who they wanted to be. They needed to focus and hold themselves accountable to grow. Brian challenged his team to focus on and develop core competencies to *assess*, *secure* and *manage* cyber security for target clients (Exhibit 6).

## Assess

*ReliaQuest*'s first step with a client was to determine the conditions of the client's security posture. In order to provide a roadmap with suggestions and a "how to" guide, it was important to get an idea of where the company stood. These assessments varied in scope from the entire environment, to specific data centers or locations, to specific technologies such as performing a health check on event management. These assessments often opened up a dialogue with customers around security, risk, and compliance. As a result of the assessment, *ReliaQuest* was then able to deliver a gap analysis from the current to an ideal security state. In addition, a roadmap was provided that gave their clients a chance to see where they stood with security, and the path to follow to attain their security goals (Exhibit 7).

## Secure

*ReliaQuest* offered their own expert engineers to go out into the field, and work side by side with the client's IT team in the ongoing battle to secure data. Brian understood that the market was congested with resellers and assessment companies all offering advice to customers on general security issues. However, when it came time to step in and help fix issues and technology specific to an organization's needs, there were few options out there that would actually do the engineering work for the customer. Engineering security solutions were an historical strength of the firm and offered a competitive advantage. *ReliaQuest* was repeatedly told that customers would pay for onsite security engineers, as they were a significant source of comfort, speed to solution, and adaptation (Exhibit 8).

## Manage

*ReliaQuest* found that getting secured was not a static state of being, but rather an ongoing battle that required consistent monitoring, optimizing, and managing. *ReliaQuest* offered monitoring, management and maintenance of customer's critical tools 24/7/365 by their certified and trained staff. *ReliaQuest*'s model was to co-manage a customer's existing technologies from the *ReliaQuest* security operations center (SOC). The key was to provide the ongoing "care and feeding" that was needed without requiring the customer to transmit their data. The SOC could provide the services while insuring that customer data remained resident in the customer systems. This also enabled *ReliaQuest* to assist the customer to co-manage the entire security environment, not just one or two point technologies (Exhibit 9).

## Operations

Each of the three core competencies required a slightly different skill set, technology and team approach. Brian understood the Assess solution very well from his consulting days. The Assess solution required technology knowledgeable consultation teams of individuals who could scour the client's information systems, and effectively and efficiently complete a detailed gap analysis with recommendations for change.

The Secure solution required extremely competent security system engineers who could be and were willing to be deployed to client sites--sometimes for extended periods. They had to be self-starters who were very capable of acting independently, and who also would raise a flag if another engineering skill set was required. Embedded in customer sites, Brian found it extremely important that they also had the interpersonal and team building skills needed to successfully implement significant changes.

As Brian and his team began to address the Manage solution, they realized that an entirely different set of talents and technology investments were required. To co-manage a customer's entire information system, the *ReliaQuest* team created a solution that absorbed enormous amounts of data, aggregated it, baked it down, and tuned out the noise for their clients. They built a SOC with hardware, software, and infrastructure to physically operate the Manage solution. They also managed communications so that clients could see thousands of alerts going off daily. And they needed to maintain strong customer facing communication to insure that alerts received the appropriate action by each customer. Otherwise, in that sort of environment, customers might readily tune out the alerts, and not behave in their own best interests. *ReliaQuest* solved this issue by force ranking the alerts, so that the security team at their client's company would know what needed their immediate attention. Brian took time to consider the mass amounts of data that would be collected at a 24/7/365 monitoring service. *ReliaQuest* would not be the first one to do this, but what could they do to focus in on the most critical data to pass on alerts to clients, and create a competitive advantage for their business?

## RQ Aware

*ReliaQuest*'s co-managed service platform was enhanced by their signature "RQ Aware" technology, which was targeted to the needs of the client. RQ Aware eliminated the noise of overwhelming numbers of alerts by using a process that force-ranked alerts, and shared only the most important alerts with the customers. The force-ranking was based upon independent analysis of the threats performed by the *ReliaQuest* algorithms, and based upon the customer's self-defined levels of data importance.

For ongoing security, the threat intelligence engine was the "big data" gatherer that pulled together alerts on malicious attacks using a variety of proprietary methods. This data was categorized and organized from a number of honeypots deployed throughout the world used specifically by the *ReliaQuest* team to gather intelligence on attacks and attackers. The results were then imported in a SIEM compatible format once the data had been aggregated by the in-house log aggregator.

## One-Stop Shop vs. Co-Managed Solutions

The cyber security industry had a large volume of managed security service providers (MSSP) that offered a one-stop shop for outsourcing security needs for firms (Zhao, Xue, & Whinston, 2013). *ReliaQuest*'s key competitive advantage over these providers was their decision not to be a company's one and only source for cyber security. Brian decided to pick and choose carefully the areas of *ReliaQuest's* expertise, and partner with other providers as necessary to address client company issues. Also, *ReliaQuest* solutions were designed to be a partnership with a co-managed platform in which *ReliaQuest* and the client company participated regularly.

Brian likened this to a NASCAR analogy:

> *"You have a racecar driver, but you don't expect him to get out and change his tires -- even if he knows how to do it. You have a pit crew where every person is responsible to do something in order to get the car back out on the road as fast as possible. ReliaQuest is the pit crew, working together with the client to assess, secure and manage their data." - Brian Murphy, CEO, ReliaQuest*

In addition, *ReliaQuest* did not market itself as a perimeter cyber security business. For Brian it was not about simply setting up a castle wall or moat around the client companies' systems and data. He insisted on an assessment method that involved going in and learning the ins and outs of every client. Brian believed: "Every client handled differently depending on their needs." One of the core competencies of *ReliaQuest* was their initial assessment when they learned where the most important data resided in the client's infrastructure, determined any weak points, and designed a roadmap to improve security optimization. The nature of this assessment was a co-managed system where *ReliaQuest* was prepared to be in it for the long run, and that the client took an active role in their own security.

Ultimately, *ReliaQuest's* strategy was to become a partner to their client, and not be the sole gatekeeper of the company's IT security. Companies had to take an active role in their security in order for this co-management to be successful. The co-managed platform allowed the customer to leverage *ReliaQuest's* secured operating center to help monitor, manage, and optimize their security environment without giving up control of their data and access to their security tools. When the work required an onsite engineer, *ReliaQuest* would send one of its many field engineers to help "on demand"--a capability that traditional MSSP's did not provide.

In Brian's experience, clients of many different sizes frequently did not have the budget, time, or experienced cyber security talent to build their own complete security infrastructure and security teams. Even organizations with the largest teams and largest expenditures frequently found it difficult to keep up with the training, development, and hiring necessary to truly fully manage the security environment without help. Those companies that attempted to go this route often found that the challenge was "educating up"--convincing senior management--on the importance of more funding for security. Many times Brian had observed C level executives survey the entire business and see large technology purchases around security, and then would not approve the necessary headcount expenditures needed to run the technologies.

Ultimately, *ReliaQuest* believed it to be important to communicate clearly with their clients about the burden placed on security professionals attempting to "doing it all yourself." For Brian, it was never all *ReliaQuest* services or nothing. Brian stated that *ReliaQuest* was happy to help clients now that wanted to experiment with new security solutions they may not purchase until sometime in the future. Often, *ReliaQuest* worked with IT and security departments to help them communicate to senior management the importance of securing specific areas of the business. With many clients, not all of the services provided by *ReliaQuest* would be utilized, but being able to co-manage alongside *ReliaQuest*, and have them there as a partner to keep the technologies optimized while advising on the plan for the future could be invaluable (Exhibit 10).

*ReliaQuest* was in the business of providing options that mitigated risk--risk to intrusion and loss of information. Persistence in the implementation of a continuous improvement plan was important nonetheless. A client that decided to initiate the assessment from *ReliaQuest*, but in order to meet budget constraints deviated from the roadmap provided by *ReliaQuest*, would dramatically increase the probability of a security failure. Ultimately, clients could easily think that they did not have the IT resources to main-

tain ongoing surveillance, and that hiring *ReliaQuest* to monitor, manage, and optimize was not an affordable option.

Ultimately, Brian believed that security was not a "set it and forget it" function in an organization. It needed to be consistently tuned and monitored. Brian used an analogy when explaining the active role a client company was expected to take.

> *"It would be like saying I have no active role in my health. I outsource everything related to my health to other people who will check my blood and manage all of the things that must be managed to stay healthy. The point is if you want to get healthy, you have to participate as well. The same applies to the process of managing cyber security, you can't just push a button and say someone else will do it all for me, it is a partnership." - Brian Murphy, CEO, ReliaQuest*

Clients of *ReliaQuest* were faced with a number of options to consider. The decision often weighed heavily on clients, as it could be the difference between securing everything and losing everything. Some companies were overwhelmed to the point of doing nothing. Brian felt this was often based on not having the understanding or the budget to bring in a firm like *ReliaQuest*. The risk here was that a company could very well lose everything, which would be more costly than to bring in *ReliaQuest* to provide a long term road map to security. Brian and his team needed to keep in close contact with companies like this as they continued to rebalance their budgets. Some companies felt that if the large companies could not stop the breaches, then they would not stand a chance, and felt helpless in the face of inevitable breaches.

Despite the bleak outlook provided by the FBI Director, who claimed everyone has been hacked whether they know it or not, Brian felt confident that the future of cyber security was bright, that awareness was at an all-time high, and the conversation was happening at all levels of commerce, government, and education. He thought that he and his company had the tools to increase visibility, and raise cybersecurity awareness throughout an organization.

With all of these services available for a client to build their own package based on their security needs, Brian still had questions. How much risk should *ReliaQuest* be willing to take with a client? How does a client manage risk when partnering with *ReliaQuest*? Was *ReliaQuest* an insurance policy? Could they guarantee zero breaches? Would they reimburse for data losses? Would they cover any business interruption costs incurred by a customer? What if the customer was ten times or one hundred times the size of *ReliaQuest*?

## Risk Management and Information Security Management

The European Union Agency for Network and Information Security provided an operational definition that explained the difference between risk management and risk assessment as major components of information security management (ISM). As generally accepted by information security experts, risk assessment has been a part of the risk management process. Risk management was a recurrent activity that dealt with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. On the other hand, risk assessment was performed at what may be considered a discrete time (e.g., once a year, on demand, etc.) to provide a temporary view of assessed risks, and create a parameter of the entire risk management process, until the next assessment (Exhibit 11) ("Risk Management," 2014).

> *"Risk management is limiting the things that you can't see or don't know about… If you can't see the problem… you know how to check for it. Risk management is based on guidelines and requirements. My problem may be different than someone else's. Risk assessment is really looking at where you are now, evaluating what your risk drivers are, evaluating your business risks…*

*what your compliance drivers are, assessing where your vulnerabilities are and building a roadmap of how you would correct those things over time. At some point there is a level of risk that everyone must be willing to accept so the key is figuring out what that level is." - Brian Murphy, CEO, ReliaQuest*

## Risk Mitigation

Brian realized that the key for *ReliaQuest*'s success, and a very important component of interaction with every one of their customers, was to incorporate a conversation on risk identification (possibility of breach, data theft, data corruption, business interruption) and risk mitigation. Brian knew that customer defenses might be breached even with the best efforts of his team and his technologies. And industry-wide, the time delay from system breach to discovery could differ greatly from event to event, and the delay was widening overall (Exhibit 13). Looking at best practices, Brian was determined to have a disciplined understanding of key aspects of risk:

- *Risk Avoidance* involved methods to decrease the likelihood of occurrence by removing a hazard, or ending a specific exposure.
- *Risk Acceptance* referred to dealing with a risk when or after it occurs. If the cost of mitigating a risk is greater than the potential loss, accepting the risk may be the most viable strategy.
- *Risk Mitigation* involved methods that reduced the severity of the loss, or decreased the likelihood of the loss from occurring.
- *Risk Transfer* could be best described as a shifting of risk from one entity to another. When a risk occurred, the losses were absorbed by another entity ("Risk Management," 2014).

If Brian believed it to be important to identify the risk response and prioritize what mitigations were best for every client company, then the response to a potential risk may have a wide variety of solutions. Ideally, this sort of dialogue with the customer would insure that resources were applied where they could most effectively address the threats, vulnerabilities, and their consequences for that company.

Brian's team found that the additional benefits of a risk management and mitigation conversation to the client company were to:

- Inform and educate the client and provide incident support.
- Provide guidance, best practices, simulation, and testing.
- Provide and operate indications, alerts, and warning capabilities.
- Provide and coordinate operation centers and teams.
- Provide and participate in information sharing, situational awareness, and information fusion activities.
- Coordinate and provide response, recovery, and reconstitution ("Risk Management," 2014).

In addition, Brian found that sound risk management led to the development of new prevention techniques, and the improvement to the overall incident management lifecycle for future attacks. Effective risk management would include the continuous feedback that led to improvement in client and engineer training and awareness, mechanisms to integrate incident lessons learned into subsequent product and services design, and improved testing procedures based on known vulnerabilities and threats ("Risk Management," 2014).

Brian also believed that constant risk management and assessment was needed across and among cyber security partners and customers as threats continued to grow and become more sophisticated, and as adversaries improved their capabilities. He was convinced that the use of these measures would reduce the

likelihood of a threat incident if they led to improved information and intelligence flows between and across the public and private sectors to support the rapid identification of emerging cyber-related threats and other circumstances requiring intervention (Exhibit 14).

## The Decision

Ironically, as Brian contemplated the medical device customer's demand for guarantees, he reflected on his own deal with his SOC building contractor. He realized that his "deal" with his SOC builder limited his recourse to the cost of materials and a chance for the builder to "make it right." Also, the contract said the builder would provide a "workman-like" product, but not be responsible if the construction interrupted *ReliaQuest*'s business. If it was a total failure, the most Brian could get back would be amounts he had paid to the construction firm.

Brian thought to himself, "Was that good enough for a cyber-security solutions provider?" Every one of his customers was under threat of more and more sophisticated attacks. The criminals only had to be right once--could ReliaQuest be perfect one hundred percent of the time? How did you take a customer's money, and still tell them they would be breached? If they were not breached, was it because no attack got through the defenses, or was it because you were unable to identify the breach? Was a breach with no sensitive data loss different than other types of breaches? By the way, how did customers distinguish sensitive from insensitive data? Did outsourcing cyber security to a solutions provider shift the liability for a security failure from the buyer to the provider? Given the size of this billion-dollar customer, could ReliaQuest even cover a loss?

How should Brian respond to the medical device customer's demand for cybersecurity guarantees?

1. *Tell the client company there were no guarantees on ReliaQuest solutions? Breaches would happen. With ReliaQuest solutions they would just happen less frequently…*

2. *Guarantee to the client that ReliaQuest would do their job and prevent breaches and data loss?*

3. *Guarantee to the client that breaches would happen, but no data would be lost. With the guarantee, should he make a promise to pay for data lost based upon the actual cost the client incurred?*

4. *Clearly with a client this big, budgets weren't really the issue. Should ReliaQuest simply triple the price or more, and provide the dedicated support demanded by the CIO and CEO?*

## References

Agrawal, M., Campoe, A., & Pierce, A. (2014). *Information security and IT risk management.* New Jersey: John Wiley & Sons, Inc.

Fraiha, S. (n.d.). *Privacy issues and monetizing Twitter*. Richard Ivey School of Business Foundation.

*Framework for improving critical infrastructure cybersecurity.* (2014) Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

*Global Security Spending to Grow 7.9% in 2014, Gartner Says.* (2014) Retrieved from http://blogs.wsj.com/cio/2014/08/22/global-security-spending-to-grow-7-9-in-2014-gartner-says/

Hkrabeepetcharat, A. (2013). IBISWorld Industry Report OD4584. *IT Security Consulting in the US*. Retrieved November 10, 2014 from IBISWorld database.

IT Sector Coordinating Council. (n.d.). Retrieved from http://www.it-scc.org/

Pelley, S. (n.d.). *FBI Director James Comey on threat of ISIS, cybercrime*. Retrieved November 25, 2014, from http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/

PWC. (2011). *Cyber Security M&A: Decoding deals in the global Cyber Security industry*.

PwC, CSO magazine, CIO magazine. (2014). *The Global State of Information Security® Survey 2014.*

PWC. (2015). *Managing Cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*.

*Risk Management & Information Security Management Systems.* (2014). Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms

Savoie, M. J. (2012). From building successful information systems: Five best practices to ensure organizational effectiveness and profitability. *Harvard Business Review Press*, 1-10.

*SIEM: A market snapshot.* (2007) Retrieved from http://www.drdobbs.com/siem-a-market-snapshot/197002909

Stallings, W. (2013). *Cryptography and network security: Principles and practice* (6th ed.). New Jersey: Prentice Hall.

*Verizon data breach investigations report (DBIR).* (2014). Retrieved from http://www.verizonenterprise.com/DBIR/2014/

*Risk Management & Information Security Management Systems.* (2014). Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems, 30*(1), 123-152. doi:10.2753/MIS0742-1222300104

Zolper, A. (Director) (2014, December 1). *Cyber security in financial services: Threats and solutions*. USF Special Guest Lecture. Lecture conducted from Andy Zolper, CISO, Raymond James, Inc, Tampa.

## Acknowledgements

This case discussion research was completed by this team of MBA students in the MUMA College of Business at the University of South Florida with significant support and contributions by Mr. Brian Murphy, President & CEO, *ReliaQuest*.

## Biographies

**Eric Biel** graduated with distinction from the College of Behavioral and Community Sciences at the University of South Florida. He was selected by the university as a Student Success profile. Eric is currently pursuing a Master of Business Administration at the University of South Florida. He has seven years of professional experience serving as the state's fiscal coordinator of a non-profit program at the University of South Florida.

**Norma Gonedes** graduated from the Queens College, City University of New York with a dual degree in political science and psychology. Norma is currently pursuing a Master's Degree in Business Administration at the University of South Florida. Norma has over ten years of professional experience in global compliance as a research analyst for Know Your Partner at Marsh, Inc., and in national corporate sales as well as international sales for Latin America at the Avis Budget Group.

**Darin Peachee** graduated with honors from the College of Arts & Sciences at the University of South Florida with degrees in both history and humanities & cultural studies. Darin is currently pursuing a Master of Business Administration at the University of South Florida. He has seven years of professional work experience serving as a data management analyst at Lakeland Regional Medical Center.

**Edgar Ramirez** graduated from Pontificia Universidad Catolica del Peru with a Bachelor's Degree in Economics. Edgar is currently pursuing his Master's Degree in Business Administration at the University of South Florida with a concentration in information systems. Edgar has five years of experience in the financial services industry and currently works at DTCC as a reporting business analyst in the IT department. Edgar is originally from Peru and has been living in the Tampa Bay area since 2004.

**Jing Yang** graduated with distinction in industrial engineering from Tsinghua University in Beijing, China. She is currently pursuing a Master of Business Administration at the University of South Florida and working as the graduate assistant for the Muma College of Business. She has eight years of professional work experience setting up China entities from Silicon-based high tech companies.

# Exhibit 1: Basic Definitions and Types of Cyber Attacks

## Basic Definitions

Information security: Commonly known as cyber security, is defined as the group of technologies, processes and practices designed to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The term cyber security is the equivalent, in a computing context, to the physical information security.[2]

Hack: Breaking into a server from a remote location to steal or damage data. Hacks generally occur when someone outside the organization attempts to take data stored on the organization's system.[3]

Data Breach: Incident in which sensitive and confidential data has been viewed, stolen, or used by an individual unauthorized to do so. Breaches generally occur inside of an organization and may be the result of malicious intent by an individual or may be the result of simple negligence.[4]

Backdoors: Consists in the access to a computer program to break into security mechanisms by the installation of another program in the back door (and that is the reason for the name).

Denial-of-service attack: Consists of getting access into a network, computer or program in order to disable them, unlike other types of attacks that are designed to access and control the system.

Direct-access attacks: The most common attack in which unauthorized user gains access to computer to compromise security.

Exploits: A piece of software that takes advantage of a software malfunction such as bug or glitch in order to cause unintended behavior to occur on computer software or hardware. [5]

[2] There is not a generally-accept orthographic rule for the word cyber security and can be either used as a single word cybersecurity or compound phrase cyber security.

[3] Harvard Business Publishing (December, 2012), BEP 191 Chapter eight, Security

[4] Ibid.

[5] Wikipedia (2014), Cyber security vulnerabilities. http://en.wikipedia.org/wiki/Computer_security

## Exhibit 2: Key findings from the 2014 Cost of Cyber Crime Study[6]

Cyber-crimes continue to be very costly: The average annualized cost of cyber-crime incurred was $12.7 million, with a range of $1.6 million to $61 million; an increase of nine percent or $1.1 million over the average cost reported in 2013.

Cyber-crimes are intrusive and common: Organizations experienced a 176 percent increase in the number of cyber-attacks, with an average of 138 successful attacks per week, compared to 50 attacks per week when the study was initially conducted in 2010.

Cyber-crimes require more time to resolve: The average time to detect a malicious or criminal attack by a global study sample of organizations was 170 days. The longest average time segmented by type of attack was 259 days, and involved incidents concerning malicious insiders. The average time to resolve a cyber-attack once detected was 45 days, while the average cost incurred during this period was $1,593,627 – representing a 33 percent increase over prior year's estimated average cost of $1,035,769 for a 32-day period.

Cyber-crimes impact all industries: Of the 17 industries included in the study, all reported to have been impacted by cyber-crime, and in the U.S., the highest annual cost per organization was reported in the Energy & Utilities and Defense industries. The average annualized cost per company in the Energy & Utilities, Technology and Retail sectors rose most significantly in the U.S. when compared to average annualized cost over the 5 years the study had been published. The retail sector alone had more than doubled in cost when compared to the average cost per breach over the five-year period.

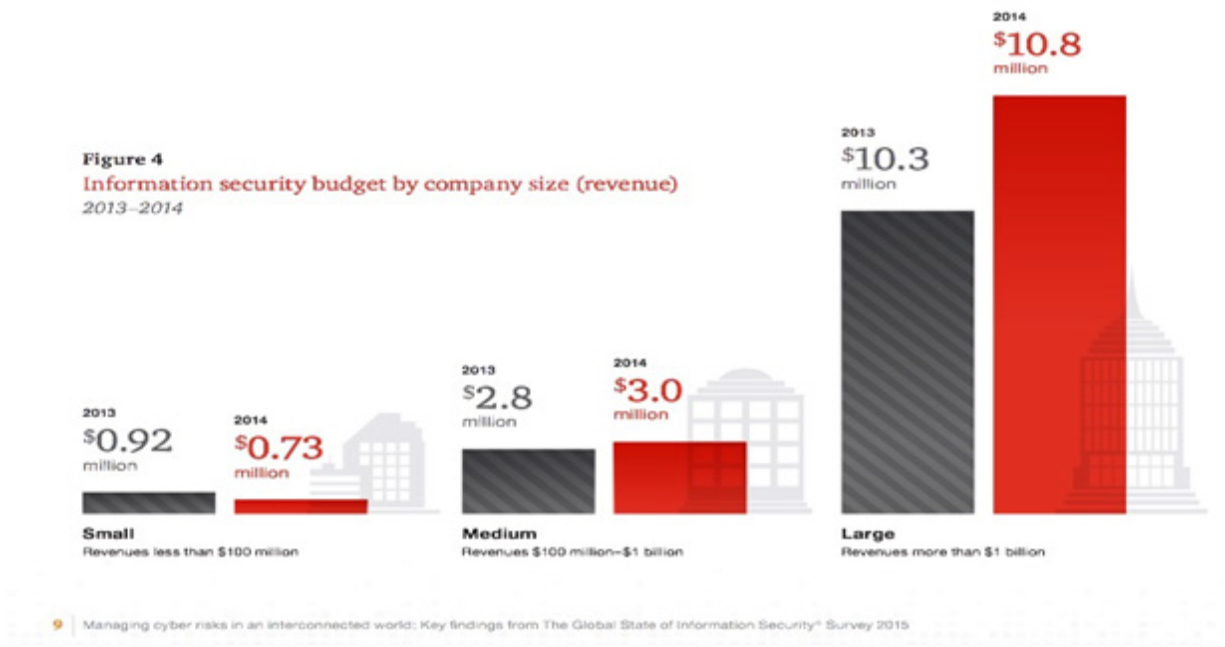
### Costly Cyber Crimes

The most costly cyber-crimes were those caused by denial of services, malicious insiders and malicious code. These accounted for more than 55 percent of all cybercrime costs per organization on an annual basis. Information theft continued to represent the highest cost to companies followed by the costs associated with business disruption. On an annual basis, information theft accounted for 40 percent of total external costs (down two percent from the five-year average), while costs associated with disruption to business or lost productivity account for 38 percent of external costs (up seven percent from the five-year average).

Recovery and detection are the most costly internal information security activities, accounting for 49 percent of the total annual internal activity cost with cash outlays and direct labor representing the majority of these costs.

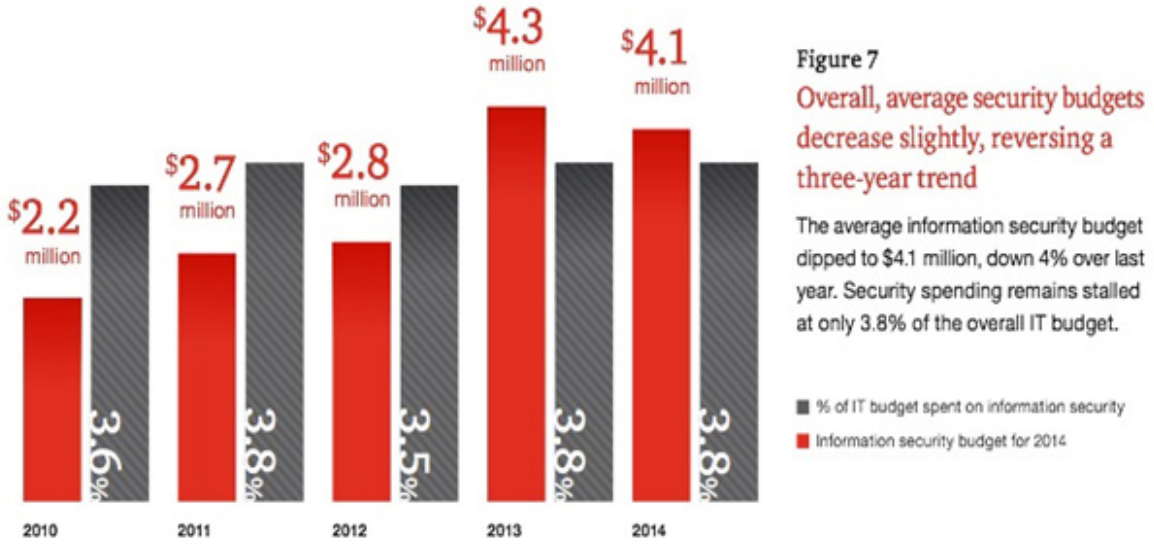
[6] Extracted from Hewlett Packard, 2014 Cost of Cyber Crime Study (October, 2014)

## Exhibit 3: Information Security Budget by Company Size



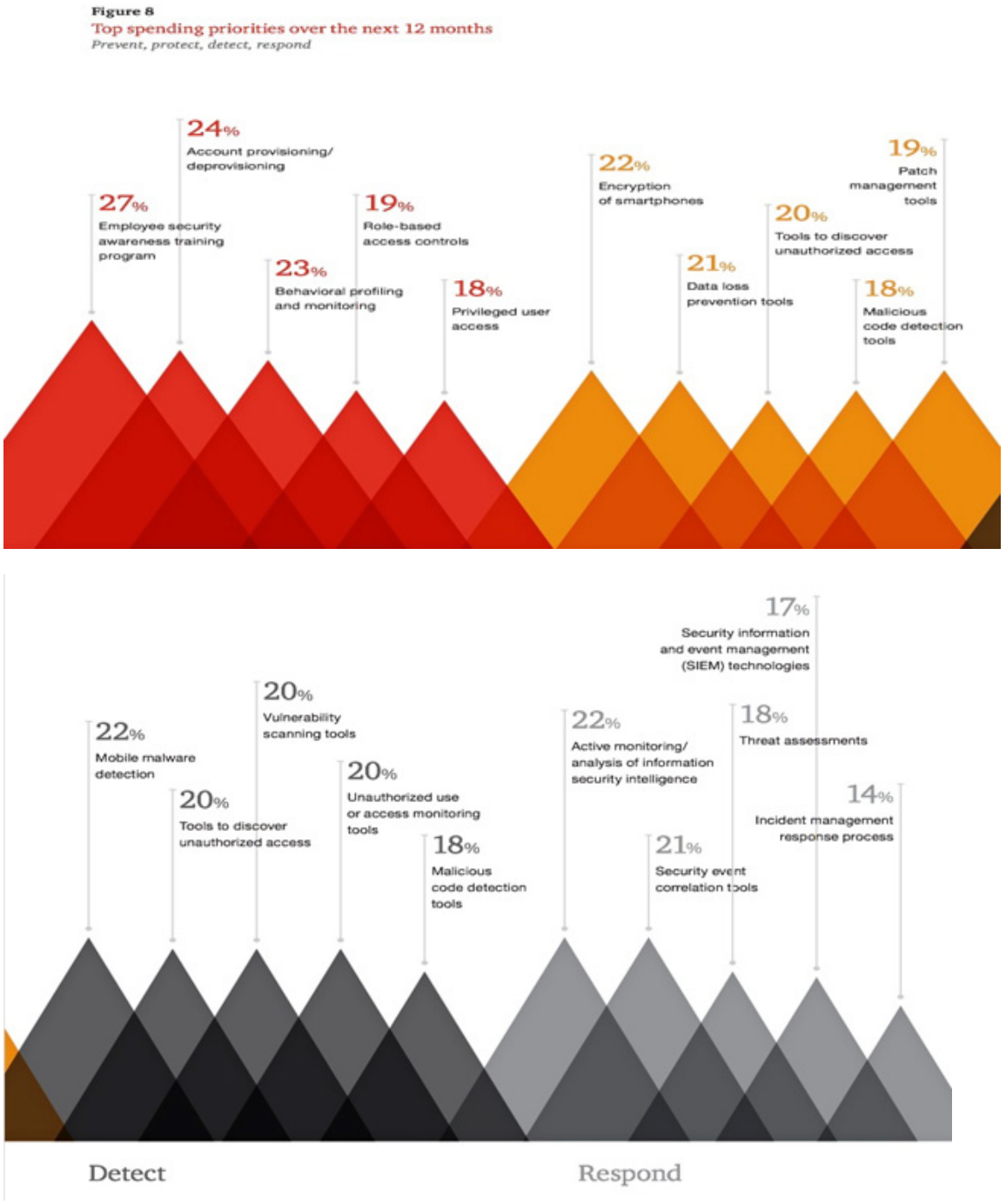

*Source:* PWC. Managing Cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015.

## Exhibit 4: Average Security Budgets Decreased Slightly in 2014




*Source:* PWC. Managing Cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015.

## Exhibit 5: Top Spending Priorities Over the Next 12 Months




*Source:* PWC. Managing Cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015.

## Exhibit 6: Stages of an Advanced Attack

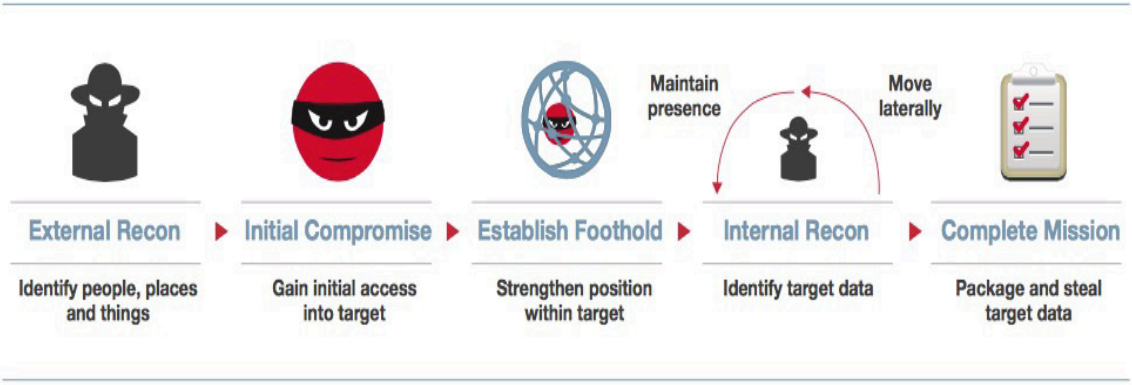
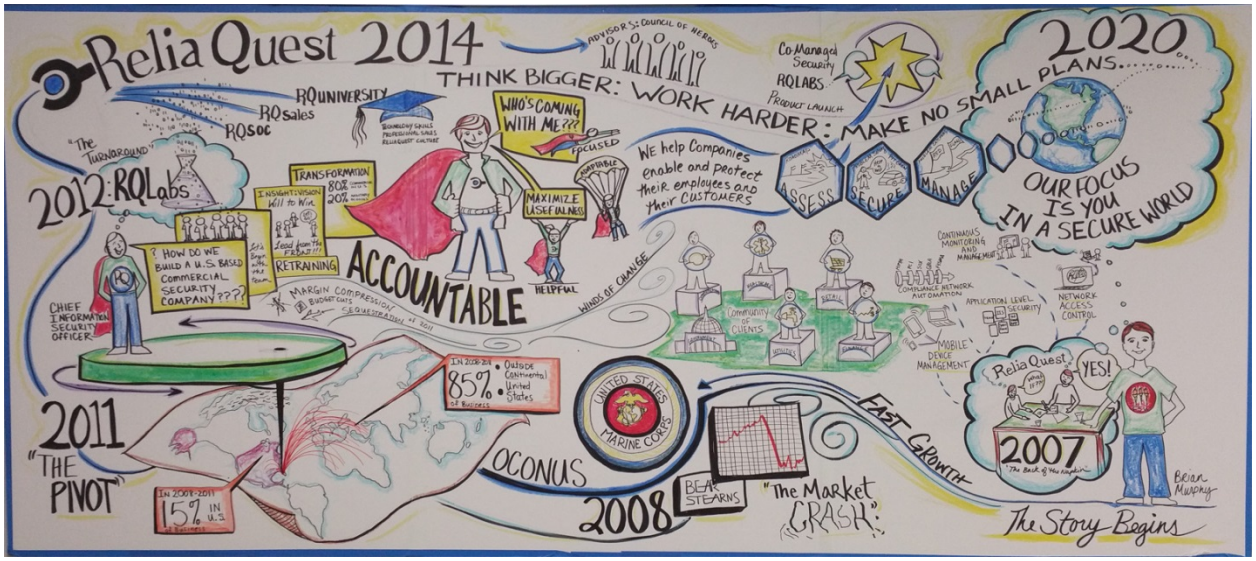



**Figure 4:** Stages of an advanced attack.

*Source:* FireEye. (2014). Cybersecurity's maginot line. FireEye Company.

## Exhibit 7: ReliaQuest Info-Graphic




*Source: ReliaQuest's* Tampa Office

## Exhibit 8: Services Offered Under "Assess"

| | |
|---|---|
| **Security Posture Analysis** | Assessment of critical infrastructure and IT controls |
| **SIEM Health Check** | In-depth analysis of current SIEM deployment |
| **Security Solution Health Check** | Firewall management solutions, email security solutions, etc. |
| **Security Planning Services** | Roadmap for security program |
| **Security Solution Selection** | Consulting on new security enterprise purchases. |
| **Critical Controls Mapping** | Maps existing infrastructure to 20 critical controls and makes recommendations |
| **Compliance Check** | Reviews current compliance status |

*Source: ReliaQuest* website: http://www.reliaquest.com/assess/

## Exhibit 9: Services Offered Under "Secure"

| | |
|---|---|
| **Resident Engineering** | Longer-term solutions for companies that need experienced engineers |
| **SIEM Optimization** | Optimization of system upgrades, tuning of sources, reconfiguration of storage, etc. |
| **SIEM Use Case & Content Creation** | Ensure source is feeding correctly and create all relevant reports, alerts, filters, etc. |
| **Security Solution Tuning** | Fully optimizing complex security solutions to produce the desired ROI |
| **Security Optimization** | Fix multiple issues while providing a longer-term roadmap with technology recommendations and enhancements |
| **Security Solution Integration** | Develop customer applications to allow older or proprietary systems to be adapted and included in the security infrastructure |

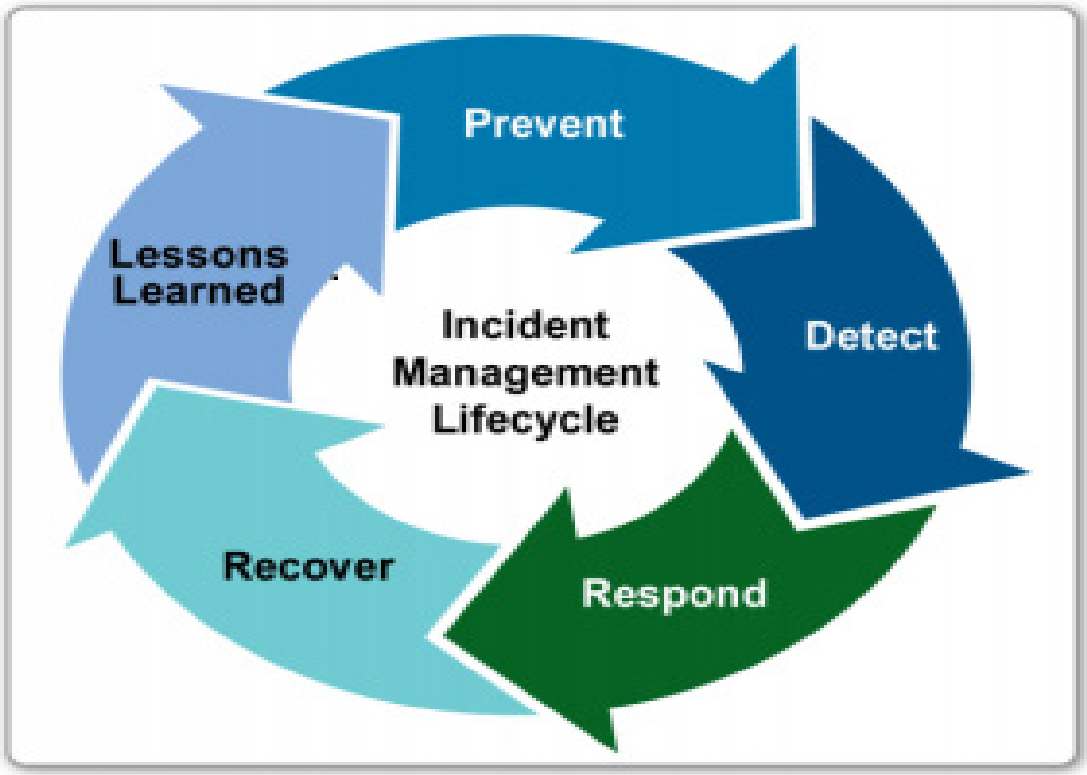
*Source: ReliaQuest* website: http://www.reliaquest.com/secure/

## Exhibit 10: Services Offered Under "Manage"

| | |
|---|---|
| **SIEM & Log Management** | Leverage existing solutions to deliver compliment monitoring and management |
| **RQ Aware** | Threat Intelligence system that gathers data information and exports into actionable use cases |
| **Continuous Compliance** | Continuous monitoring networking configurations from all layer-3 devices |
| **Network Access Control** | Assess network for vulnerabilities, unwanted access, and proper network segmentation |
| **Application Security** | Assist of fully manage security of your applications |
| **Perimeter Security** | Manage existing perimeter security investments or deploy and monitor technology |
| **Vulnerability Management** | Leverage leading technologies to prioritize remediation of results |
| **Configuration Management** | Managed or co-managed, hardening your environment greatly preventing attacks |
| **Endpoint Management** | Protect your infrastructure to the edge with turn-key services helping protect the most valuable assets you have |

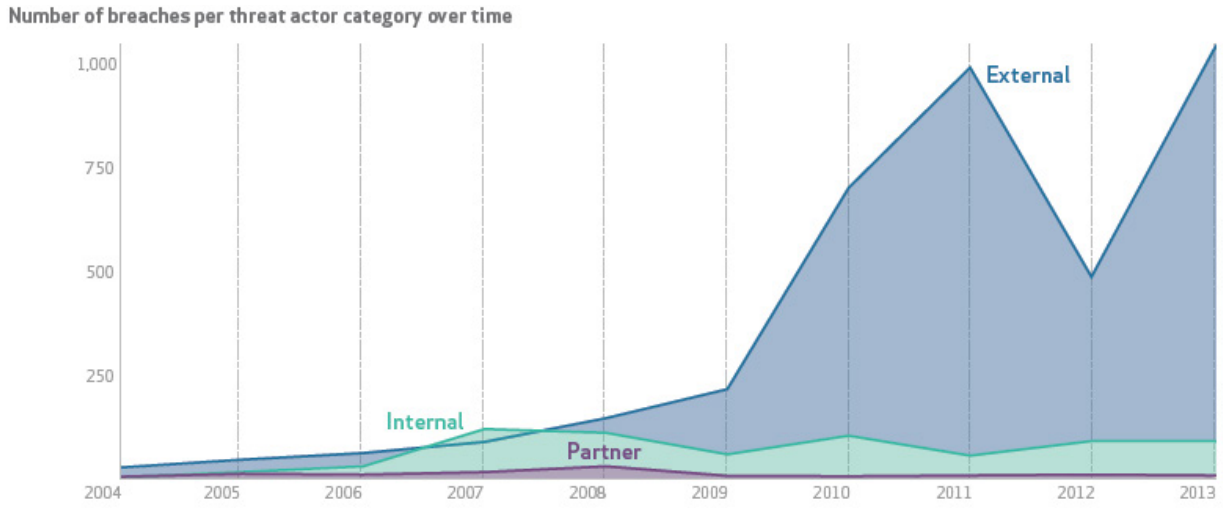
*Source: ReliaQuest* website: http://www.reliaquest.com/manage/

## Exhibit 11: Incident Management Lifecycle



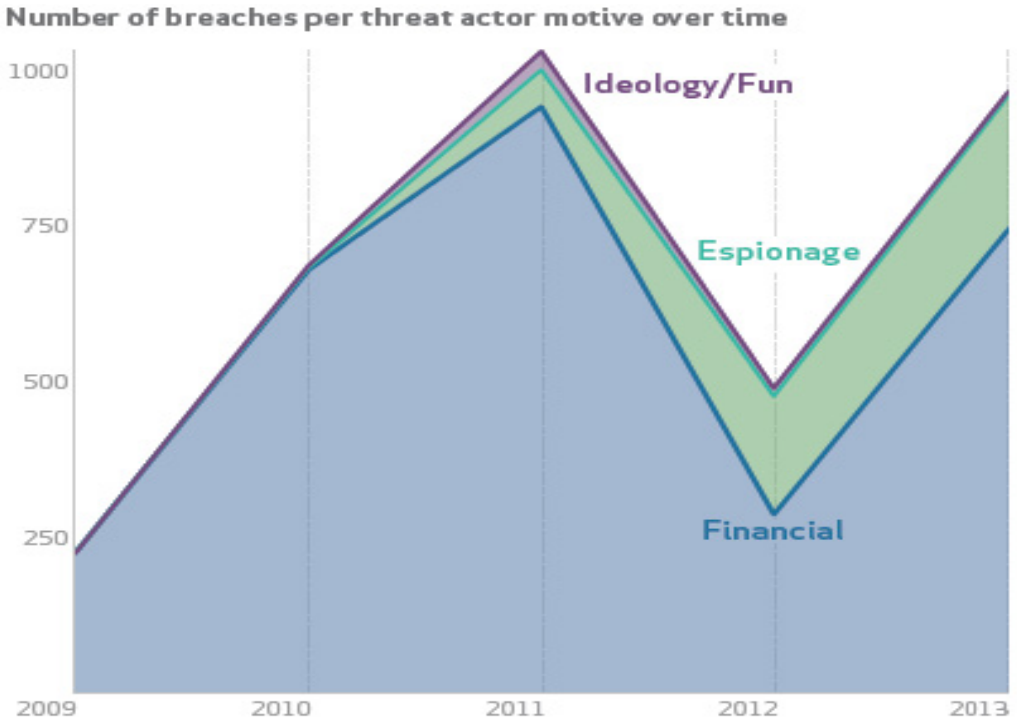

*Source:* IT Sector Coordinating Council. (n.d.). Retrieved from http://www.it-scc.org/

## Exhibit 12: Number of Breaches per Threat Actor Category Over Time



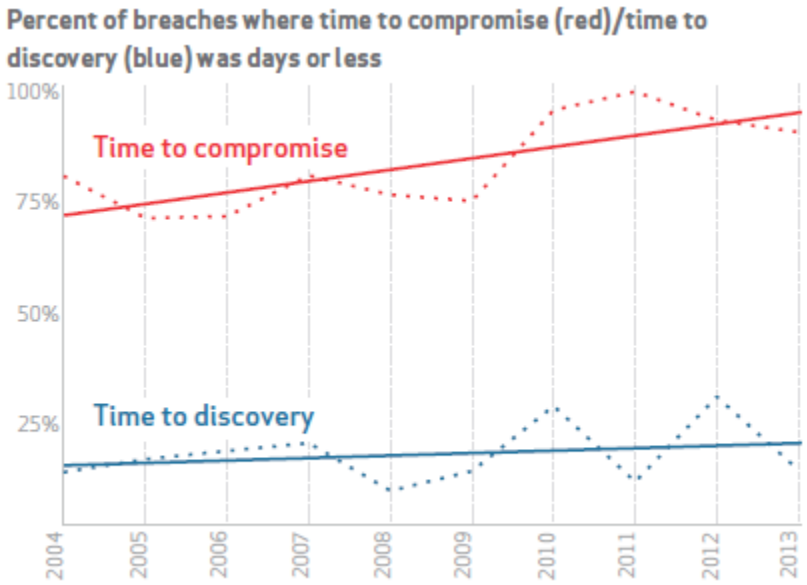

*Source: Verizon data breach investigations report (DBIR).* (2014). Retrieved from http://www.verizonenterprise.com/DBIR/2014/

## Exhibit 13: Number of Breaches per Threat Actor Motive Over Time




*Source: Verizon data breach investigations report (DBIR).* (2014). Retrieved from http://www.verizonenterprise.com/DBIR/2014/

## Exhibit 14: Time Delay From System Breach to Discovery




*Source: Verizon data breach investigations report (DBIR).* (2014). Retrieved from http://www.verizonenterprise.com/DBIR/2014/