Cyber Failures – Who's to Blame?

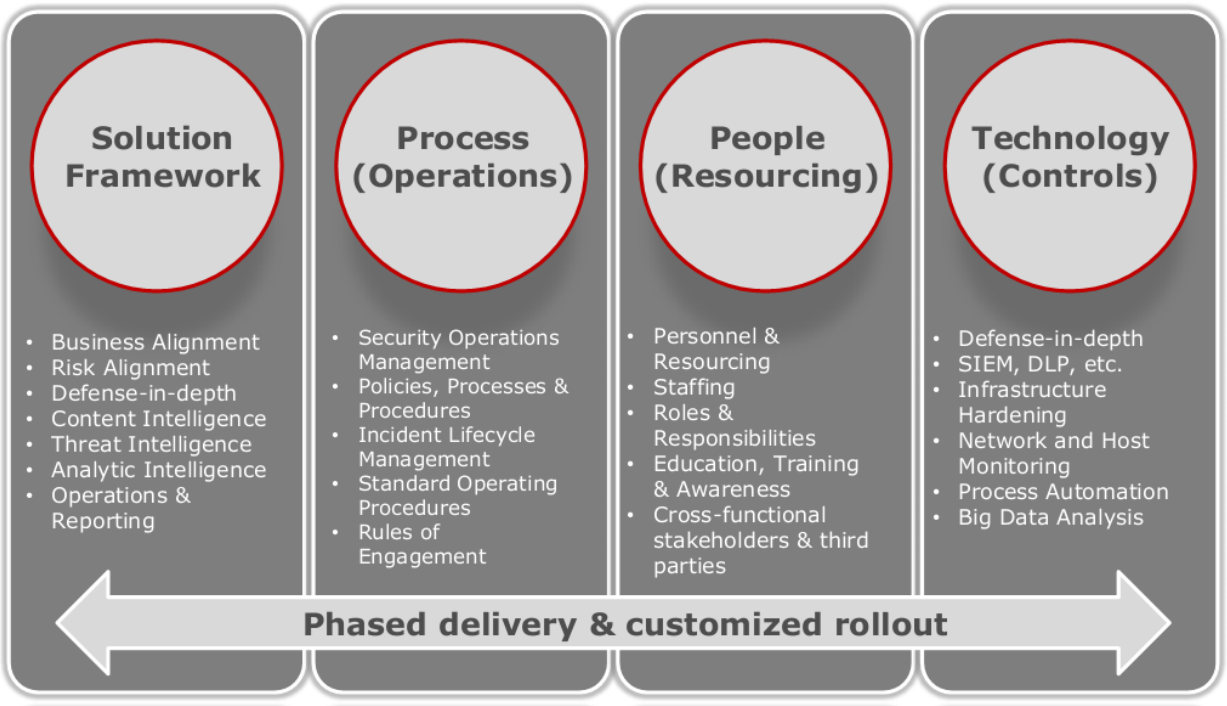
Lead Analyst: Cal Braunstein

Cyber security is back in the news. Last month the Internet security firm Mandiant Corp. issued a report that linked China' People's Liberation Army to hundreds of thousands of cyber attacks across the globe, including U.S. corporations and government agencies. Only 37 percent of the organizations discovered the breach internally, the report stated. Last week U.S. intelligence officials told a Senate hearing that the nation is vulnerable to cyber espionage, cybercrime, and outright destruction of computer networks across all industries and sectors and put at risk critical infrastructures. The volume of total stolen data is staggering, even if one only looks at China's activities. In March 2011, a single cyber intruder stole 24,000 files from a defense industry computer network. Cyber attacks can expose customer information, steal intellectual property, destroy databases, and more, all of which could put a company at severe business risk. If this were to occur to a company, who is to blame for the failure to prevent the attack?

RFG has noted that past failures have led to the departure of IT executives, especially the Chief Information Security Officer (CISO) or whomever is responsible for security. However, that should not necessarily be the case. Multiple layers of management are responsible for cyber security and breach prevention and in many cases it is up to IT to make the other parties aware of their responsibilities and to act on them. To put it another way, if IT executives do not ensure the involvement and shared burden with other corporate executives, then IT will take the blame.

The below graphic (Figure 1) shows the components of a next-generation security operations center (SOC). IT may look like an IT-only roadmap but it is not. The upgrading of the existing

Figure 1. Next-generation SOC Components



Source: RSA 2013 Conference

solutions to encompass all of the elements identified in Figure 1 will require increasing the IT security budget and a redefinition of security goals, policies and responsibilities. For example, according to the Carnegie Mellon CyLab 2012 Governance survey less than one-third of boards of directors and senior management are exercising appropriate governance over the privacy and security of their digital assets. If the senior executives are not engaged in ensuring the protection of assets, then IT most likely is underfunded in its attempt to reduce the cyber risk exposure and will take the fall when a major breach is identified.

Assigning Responsibilities

While it is not IT's job to tell CEOs and boards what their roles are, IT executives can bear the brunt of the blame if they do not outline *in writing* what they expect from senior management and the board. RFG recalls a 9/11 World Trade Center incident where IT executives' jobs were on the line because they had not implemented certain disaster recovery techniques. The IT executives were able to point to a presentation they made to senior management requesting the funds but were denied. By having the proof that they asked for but failed to receive the funding, the IT executives were able to show the failure was a shared one and no jobs were lost. Thus, IT executives need to make it clear to all what is expected.

At the board level there should be a risk committee that is responsible for all risk management, including cyber risk. Moreover, best practices find boards should address the following five areas:

- regularly reviews and approves top-level policies on privacy and IT security risks
- regularly reviews and approves roles and responsibilities of lead personnel responsible for privacy and IT security
- regularly reviews and approves annual budgets for privacy and IT security programs separate from IT budgets
- regularly reviews and approves cyber insurance coverage
- regularly receives and acts upon reports from senior management regarding privacy and IT security risk exposures.

These efforts can be done by the full board or by a risk committee that reports to the board. Some boards may have assigned this role to the audit committee but, while it is good that it is addressed, it is not a perfect fit.

The CEO should be participating in the board discussions and be assisting in the preparation of the review materials. Like the board, the CEO has a fiduciary responsibility to shareholders to protect the company's assets from undue risks. They should be involved in cyber security governance and decision-making on an ongoing basis and not shunt it off to Chief Risk Officers (CROs), Chief Security Officers (CSOs or CISOs) and/or IT executives. CEOs and other senior executives should also ensure privacy and security programs are aligned with each business unit's requirements and that the risk probability and exposures are reasonably known and reduced to an *acceptable level*. It is important that all parties understand that zero security risks are not possible anymore (nor would the expense be worth it if attainable); what is important is to agree upon what level of risk exposure is acceptable, budget for it, and implement initiatives to make it happen.

IT executives should also ensure that the appropriate risk and security executive positions, roles and responsibilities are defined, and the jobs filled. Figure 2 provides a sample matrix of 15 key areas of privacy and security risks that must be governed and monitored by various executives. (Not all companies will have each of the positions in place, while some might have multiple.)

Figure 2. Risk/Responsibility Matrix

RISK / RESPONSIBILITY MATRIX					
ROLE->	CRO	CISO	CSO	Audit	Compliance
RISK AREA					
Applications					
Backup/Recovery					
Change Management					
Corporate and Cloud Infrastructure					
Data and Information					
DR/BC					
External Infrastructure					
Human Resources					
Operational					
Policy and Procedure					
Privacy and Security					
Projects/PPM					
Records Retention					
Transactional					
Vendor Management					

If IT executives can persuade senior management to put all the appropriate budgets, parties and responsibilities in place, then there is a good chance that the company can achieve an acceptable level of risk and the risk will be a shared activity.

RFG POV: Cyber security is a competitive issue, as the perception that the organization is a trusted business is key to loyalty and continued attainment of business goals. Successful cyber security risk management is not solely an IT challenge or responsibility. IT executives should work with boards, CEOs, and senior management to get the appropriate funding, governance, personnel, policies, procedures, roles and responsibilities in place across the enterprise. Moreover, the bar for effective security operations gets raised year-over-year. Next-generation cyber security initiatives require the implementation of big data, context and incident management capabilities, monitoring, remediation, and response management along with prevention programs. Additionally, the cyber security management team should be sending the message out to customers, business partners, contractors, employees, shareholders, and suppliers that the company is committed to being a trusted partner. The executives should also be advising everyone that it expects the same level of commitment to cyber security by all those with whom they work. If all the cyber security team members keep their eye on the ball, then the breaches will be containable and within the expected acceptable levels of risk and there will be no one to blame.