Achieving Cyber Resilience

By Garin Pace, Anthony Shapella and Greg Vernaci

AIG

Cyber security has become the single most important risk to company Boards of Directors around the world. This is not a surprise – the global economy has become highly networked and depends on continuous, secure and uninterrupted data flow. The highly networked environment presents tremendous opportunities for enterprising firms, but this opportunity brings its risks. For example, recent high-profile attacks have targeted point-of-sale terminals at Target, Home Depot and Staples, server software at JP Morgan and employee databases at Sony. In the face of such complex risks, what can a company do to protect itself?

The first, and most important step, is to proactively carry out standard systems hygiene. The Center for Internet Security suggests that five simple steps can prevent up to 80% of cyber attacks. The steps include:

- Maintaining an inventory of authorized and unauthorized devices
- Maintaining an inventory of authorized and unauthorized software
- Developing and managing secure configurations for all devices
- Conducting continuous (automated) vulnerability assessment and remediation
- Actively managing and controlling the use of administrative privileges[1]

Recognizing this, the National Institute of Standards and Technology (NIST), working under executive order of the President of the United States, developed a common cyber security framework that provides a roadmap for companies to implement standard security practices.[2] The UK has also implemented a similar framework that it calls Cyber Essentials.[3] Clearly, standard practices will help companies improve their defenses and prevent the bulk of cyber security events.

Cyber Resilience Planning

While standard hygiene is a start, it simply cannot prevent all attacks. As such, leading firms are moving beyond prevention and focusing on resilience.[4] This can be achieved by developing a "cyber resilience" action plan for responding when an attack occurs. A plan is best developed by a cross-functional working group of senior managers (Sales/Marketing, Operations, IT, Finance, Legal, Risk, HR) that meets regularly to discuss cyber security, monitor evolving internal and external threats and model and analyze hypothetical attacks. A good resilience plan will detail roles and responsibilities, external parties that will assist with remediation, communication and crisis management plans and operating strategies for various types of events. Having an action plan in place prior to an event has been shown to dramatically reduce the cost, time to recovery and reputational damage of a breach.

It is important to appoint a strong leader to chair the working group. The chairperson is often the firm's Chief Information Security (CISO), Chief Information (CIO) or Chief Technology Officer (CTO). He or she regularly reports the group's work to the Board of Directors (or a designated sub-committee) to ensure that all parties understand the cyber security risk profile, potential threats and planned strategy for breach response. The group may also serve as the decision making body to weigh investments in systems security and other risk mitigation strategies. Last, and most importantly, the group should foster an on-going and active dialogue between the firm's senior executives so that all parties are prepared to respond and on the same page when an event occurs.

1 http://www.nationaldefensemagazine.org/archive/2014/May/Pages/NewCyberHygieneCampaignSeekstoCurtailAttacks.aspx

2 The framework can be accessed here: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

3 The scheme can be accessed here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

4 CRO Forum. Cyber Resilience – The Cyber Risk Challenge and the Role of Insurance. http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/

Crafting the Plan

Once the group is established, the chairperson can begin work on the plan. First, it is important to map out the firm's cyber risk profile. While this sounds daunting, our experience suggests that it is far more manageable once the group gets started. A recent Verizon study notes that roughly 95% of all cyber attacks can be explained by nine basic patterns.[5] Studying these patterns is a good way to identify the types of attacks that cause loss and tailor one's activities to those modes that are most relevant. Some groups find that having an external cyber security expert facilitate the first meeting is helpful.

After attack modes are well understood, the group can work on mapping the risk landscape using a scenario-based approach. Scenarios are very effective because they challenge the leadership team to think deeply about and discuss possible attack modes, targets, vulnerabilities and impacts. A visual map can be used to line up the various "nodes" in the attack chain. The following diagram can be used as a prototype to get the group started and generate a number of scenarios.

Threat Region	Threat Agent	Motive	Attack Method	Victim	Assets	Impact	Response	Insurance Product
Asia-Pacific	Government	Financial Gain	Trojan Horse	Financial Institution	Social security numbers	Asset impairment	Public relations	General / Excess Liab
Eastern Europe	Hacktivist	Intellectual Capital	Unpatched Software	Retailer	Credit card numbers	Reputational damage	Crisis management	Crime
Western Europe	Professional Criminal	Business Disruption	Worm Install	Healthcare Provider	Health records	Stock price decline	System restoration	Prof Ind / E&O
Middle East	Rogue Employee	Ideology	Card Skim	Stock Exchange	Trade secrets	Service interruption	Customer notification	Directors & Officers
United States	Cyber Terrorist	Revenge	Denial-of-Service	Utility	IT infrastructure	Bodily injury	Forensic investigation	Stand-alone Cyber
...	...	Entertainment	Social Engineering	IT/Software Firm	Physical plant	Data loss	Credit monitoring	Property
		Espionage	Laptop theft	Manufacturer	Account Information	Lost revenue	SEC disclosure	Aviation
		...	...	...	...	...	...	...

We've found that an easy way to "seed" the scenario library is to consider narratives of actual events and swap in the company's name and details. Then, one can iterate on that scenario by changing various nodes i.e., threat regions, threat agents, motives, attack methods, assets, impacts etc. The key to this step is to identify a robust set of possible events and discuss the likelihood and impact of each. Narratives with higher likelihood and / or impact can be prioritized first and risk mitigation strategies can be discussed across the group. The cross-functional discussion is critically important – strategies should consider all parties and their action steps from front-line sales people, to the customer service department, to operations and systems to finance, accounting and human resources.

Risk Assessment/Measurement

The next step in the process is risk assessment and measurement. This is often the step that is most daunting to the executive team. How can the group accurately assess the potential impact of a major event or data breach? The key here is to avoid analysis paralysis – getting rough figures down on paper and discussing them is more important than highly precise estimates. Further, rough estimates can be compared against external benchmarks of actual events. For example, if the Target breach happened at our firm – would the cost be higher or lower? By how much?

Fortunately, a growing data set is emerging that can help companies estimate the cost of a major cyber event. Some firms have analysts in the IT or Finance department collect information on events that have occurred and

5 http://www.verizonenterprise.com/DBIR/2014/

build a database out of this information. For example, by searching Securities and Exchange filings,[6] one can find the following information about the Target breach:

- Attack duration: 20 days (11/27 – 12/17)
- Attack method: malware installation on point-of-sale transaction system
- Attack location: U.S.-based stores
- Assets compromised:
  - 40 million credit and debit card account profiles
  - 70 million guest information profiles (names, mailing/email addresses, etc.)
- Estimated cost: ~$250 million gross and ~$160 million net

These data points can serve as a reference point to estimate the total cost of an event. Some analysts also consider a cost-per-record breached metric. For example, in rough terms $250 million of costs divided by approximately 40 million credit and debit card records suggests a per-record cost of $6.25. This metric allows one to compare costs across events and devise scenarios of varying levels of severity. Again the most important objective is to develop rough estimates rather than achieve perfect precision.

Risk Mitigation

Risk mitigation can take many forms. The most effective is to invest in defenses for the attack modes and assets that are most at risk. For example, if a company determines that its greatest threat is malware installations, to point-of-sale software systems, directed by domestic operatives, via vendor access rights, then it might consider investments in end-to-end encryption, Application White Listing (AWL), File Integrity Monitoring (FIM), system access software, vendor access controls and regular reviews of all vendor access logs.

While investing in prevention is paramount, not all attacks can be fully mitigated. For these events, cyber insurance is critically important. Cyber insurance provides contingent capital and expert assistance in the event of a cyber attack or data breach. The insurance industry has tailored a suite of products that help companies quickly restore their operations and pay financial obligations. Some cyber policies also include risk management and loss prevention services which can aid companies in assessing and mitigating their exposure to events before they occur.

A cyber policy can respond to both the liability, as well as the first-party direct costs associated with a cyber event. Some examples of first-party costs include forensic expenses, notification costs, credit or identity monitoring and loss of income from a network interruption. From a liability perspective, a cyber policy may also respond to regulatory and administrative actions, including fines and penalties arising out of the event. The cyber policy can be customized and coverage offerings can be added or removed based on the company's risk profile.

Increasingly, companies are reviewing other insurance purchases to ensure that they understand where there may be coverage or a potential gap. Some companies may purchase more Directors and Officers liability insurance to protect against shareholder claims of negligence following a breach.

6 http://www.sec.gov/Archives/edgar/data/27419/000002741914000036/tgt-20141101x10xq.htm

Additionally, some infrastructure and utility companies are reviewing their property, casualty and business interruption coverage to ensure that sufficient protection exists in the event of a cyber-driven infrastructure attack. While recent attacks have focused more on consumer points-of-sale, current geopolitical factors and a recent cyber attack on a German iron plant [7] suggest that this type of exposure cannot be ignored.

In reviewing one's coverage, it is important to note that not all policy types will respond to loss. For example, Insurance Services Office, Inc. (ISO) in the United States recently specified that its standard general liability policy excludes data and privacy losses from a cyber attack. As such, companies should consider a stand-alone cyber policy or supplemental coverage. Some insurance companies are offering new products that will "drop down" and provide coverage if cyber risks are specifically excluded from underlying general liability and property policies, as well as excess coverage to protect the company against larger losses, e.g. AIG's CyberEdge PC®.

Tying It All Together

In sum, digital assets and information networks are critical to business success. Protecting these assets is top-of-mind for Boards of Directors and senior executives at companies across the world. The first step to improving the cyber risk framework is to ensure that standard cyber hygiene is properly addressed. This will mitigate many cyber attacks, but simply cannot prevent all of them. As such, companies should focus on cyber resilience and a plan for action is essential to have in place before a breach occurs. Developing this plan can be achieved by assembling a cross-functional working group of senior managers and working to define the firm's cyber risk profile, design potential scenarios, measure the impact and size up mitigation strategies. Most importantly, companies should focus on getting started – a rough plan with crude measurements is perfectly OK. The journey to cyber resilience has to start with a single step.

For a more in-depth read on cyber risk resilience refer to the CRO Forum's recently published paper: *Cyber Resilience – The Cyber Risk Challenge and the Role of Insurance.*[8]

7 http://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/

8 http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/

Bring on tomorrow

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 100 countries. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIG_LatestNews | LinkedIn: http://www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties.

This document does not constitute an offer to sell any insurance coverage or other products or services described herein. We do not provide legal, credit, tax, accounting or other professional advice, and you and your advisors should perform your own independent review with respect to such matters as they relate to your particular circumstances and reach your own independent conclusions regarding the benefits and risks of any proposed transaction or business relationship.

02/20 SP1158Y