NEWSLETTER
RISK MANAGEMENT

THE GENEVA ASSOCIATION

No. 55, February 2015

Achieving Cyber Resilience

By Garin Pace, Anthony Shapella and Greg Vernaci[+]

Cybersecurity 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 J.P. 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 carry out standard systems hygiene proactively. The Center for Internet Security[1] suggests that five simple steps can prevent up to 80 per cent of cyberattacks. The steps include:

- maintaining an inventory of authorised and unauthorised devices;
- maintaining an inventory of authorised and unauthorised 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.[2]

Recognising this, the National Institute of Standards and Technology (NIST), working under an executive order of the President of the United States, developed a common cybersecurity framework that provides a roadmap for companies to implement standard security practices.[3] The U.K. has also implemented a similar framework that it calls Cyber Essentials.[4] Clearly, standard practices will help companies improve their defences and prevent the bulk of cybersecurity 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.[5]

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 cybersecurity, monitor evolving internal and external threats, and model and analyse hypothetical attacks. A good resilience plan will detail roles and responsibilities, external parties

[+] Garin Pace is Head of Underwriting Excellence, Cyber for the US & Canada at AIG; Anthony Shapella is Director of Risk Aggregation, AIG; Greg Vernaci is Head of Cyber for US & Canada, AIG.

[1] http://www.cisecurity.org/

[2] http://www.nationaldefensemagazine.org/archive/2014/May/Pages/NewCyberHygieneCampaignSeekstoCurtailAttacks.aspx

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

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

[5] 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*

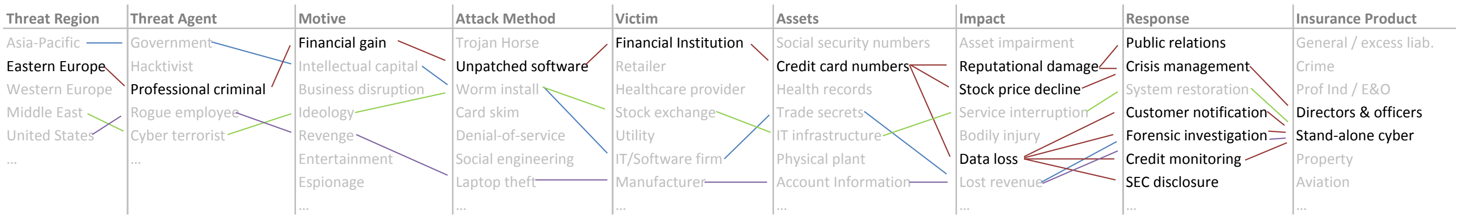
that will assist with remediation, communication and crisis management plans and operating strategies for various types of events. Having an action plan in place *prior to an event* has been shown to dramatically reduce the cost, time to recovery and reputational damage of a breach.

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 subcommittee) to ensure that all parties understand the cybersecurity 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 are on the same page when an event occurs.

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 per cent of all cyberattacks can be explained by nine basic patterns.[6] 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 cybersecurity 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 prioritised 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 for 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

[6] http://www.verizonenterprise.com/DBIR/2014/

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 build a database out of this information. For example, by searching Securities and Exchange filings,[7] 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:**
  - 40m credit and debit card account profiles
  - 70m guest information profiles (names, mailing/email addresses, etc.)
- **Estimated cost:** ~USD 250m gross and ~USD 160m net.

These data points can serve as a yardstick for estimating the total cost of an event. Some analysts also consider a cost-per-record-breached metric. For example, in rough terms, USD 250m of costs divided by approximately 40m credit and debit card records suggests a per-record cost of USD 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 defences 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 cyberattack 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 that can aid companies in assessing and mitigating their exposure to events *before they occur*.

A cyber policy can respond to both the liability and 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 customised 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. 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

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

consumer points-of-sale, current geopolitical factors and a recent cyberattack on a German iron plant[8] 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 U.S. recently specified that its standard general liability policy excludes data and privacy losses from a cyberattack. 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 towards improving the cyber risk framework is to ensure that standard cyber hygiene is properly addressed. This will mitigate many cyberattacks, 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.*

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