Environ Syst Decis
DOI 10.1007/s10669-013-9474-1

PERSPECTIVES

Cyber first aid: proactive risk management and decision-making

Ben Sheppard · Mary Crannell · Jeff Moulton

Abstract Public and private organizations need a robust approach to prepare, respond, and recover from cyber-attacks. This perspective article will refer to such an approach as *Cyber First AID*—adaptable, integrated, and deliberate. *Adaptable* describes that one size does not fit all; *Integrated* means the effort is throughout the organization; and *Deliberate* describes plans that are reviewed periodically and practiced, in which all members of the organization know their respective roles and responsibilities. The article outlines a decision-making process for how to minimize the impacts of cyber threats, maintain stakeholder and customer confidence, and help organizations to adaptively manage and respond to cyber threats in rapidly changing cyber environments.

Keywords Decision-making · Cyber-attacks · Resilience · Organizational behavior · Preparedness · Response · Recovery

B. Sheppard (✉)
Institute for Alternative Futures, 100 North Pitt Street, Alexandria, VA 22031, USA
e-mail: ben.sheppard.uk@gmail.com

M. Crannell
Idea Sciences, Inc., 205 The Strand, Alexandria, VA 22314-3319, USA

J. Moulton
Information Operation and Program Development, Georgia Tech Research Institute, 400 W. 10th Street, N.W., Atlanta, GA 30332, USA

1 Introduction

Organizations cannot afford to treat cyber threats the same as natural disasters. The potential losses are high, with extensive economic and reputational harm and even fatalities. Given the pervasive and growing cyber threat and the need for organizations to be proactive and resilient, effort toward a robust risk management strategy for organizational preparedness is a logical step—what can be called a Cyber First AID plan—Adaptable, Integrated, and Deliberate. *Adaptable* describes that one size does not fit all; *Integrated* means the effort is throughout the organization; and *Deliberate* describes plans that are reviewed periodically and practiced, in which all members of the organization know their respective roles and responsibilities. Such a risk management plan should help the organization to minimize the damage, maintain stakeholder and customer confidence, and adaptively manage and respond to the threat.

High-profile, high-loss instances of industry vulnerabilities are increasing. The hack attack on Sony's online gaming networks, including PlayStation and the theft of 77 million credit card numbers in April 2011, came at a cost of $170 million for technical fixes and a "Welcome Back" campaign to lure customers back (Potter 2011). The final figure may be far higher at $1–2 billion when taking into account losses from stolen personal information and legal action (Strategic 2011). Sony's slow response to acknowledge the attacks and lack of transparency contributed to the loss and the reputational damage that also led to stock losses. Similarly, a cyber-attack on the discount site LivingSocial in April 2013 forced it to lock out customers after 50 million account details were stolen. Many customers did not reset their passwords—instead deciding to leave the site altogether (Heath 2013). The

Published online: 16 October 2013

attack contributed toward a $34 million first-quarter loss in 2013 (Heath 2013).

A cyber-attack on Saudi Arabia's national oil company Aramco in August 2012 that damaged approximately 30,000 computers demonstrated a sophisticated attempt at stopping national oil and gas production (Reuters 2012). More ominous is an attack strategy called hardware hacking where critical circuitry is compromised at the manufacturing or supply chain level to command components to either fail or reroute data to third parties without the users or manufacturers knowledge according to preprogrammed settings. China is thought to be behind building in backdoor hardware and firmware vulnerabilities in Lenovo equipment that allows attackers to remotely access devices (Curtis 2013). After British intelligence agencies found the Lenovo vulnerability during routine security checks, government departments in the USA, UK, Canada, New Zealand, and Australia now prohibit the use of the Chinese company's equipment for classified information (Curtis 2013). These cases illustrate the scale of financial damage and security implications that cyber-attacks cause.

Overreacting to a real or perceived cyber threat can be equally devastating. In 2012, the US Economic Development Administration (EDA) went almost 12 months without Internet communication with regional offices, and desktops, laptops, servers, and printers worth $175,000 were destroyed because the agency misinterpreted a common malware infection as a sophisticated cyber-attack (Rein 2013). An Inspector General report later found a combination of inexperienced IT staff and lack of communication contributed to the outcome. In a time of fiscal austerity, EDA required $1.1 million to purchase new computers, replace networks, and acquire essential temporary office equipment (Rein 2013).

While concerns of the potential damage that cyber-attacks can cause are growing, governments and multinational institutions like the European Union are struggling to provide a comprehensive cyber approach. It is up to organizations to take the lead in developing their own cyber-defense and response capabilities. There are some promising public–private sector initiatives. For example, the UK's cyber security information sharing partnership (CISP) pulls together the expertise of the Britain's government communication's headquarters (GCHQ), internal intelligence group MI5, and government to make available their expertise to businesses (Reuters 2013). In addition, the Defense Cyber Protection Partnership brings together defense contractors like BAE Systems, Rolls-Royce, BT Group, Lockheed Martin, Hewlett Packard, and others to engage the British government in sharing information on how to recognize and address cyber threats. In the USA, the Department of Homeland Security's private sector office engages with businesses and trade associations and promotes public–private partnerships.

2 Industry cyber risk tolerance

Industry arguably has a tendency to perceive cyber-attack losses like those that occur following a natural disaster. Though it is becoming increasingly unacceptable for cyber-attacks to be viewed as similar to preparing and responding to natural disasters, the vulnerability and consequences of natural disasters are more easily understood and contained as events are generally concentrated to certain geographical areas, making it easier to map out their probability and severity. In the case of extreme weather events like hurricanes and tornadoes for example, forecasting techniques on timing, severity, and duration provide sufficient input to characterize and respond to risks to maintain business continuity. While risk characteristics of earthquakes do not lend themselves to predictability, they can be understood in terms of what geographic areas are prone to earthquakes, their potential severity, and what building structures are required to survive.

Although man-made disasters like terrorism are hard to predict—when, where, and by what means an attack may take place—installation and maintenance of geographically dispersed backup IT structures and human resources provide organizations with a degree of resiliency.

Cyber-attacks possess unique risk characteristics. They can be insidious and systemic. Unlike the geographic limitations afforded by natural disasters and terrorism, the severity and specificity of cyber-attack events are harder to anticipate. The potential costs of an attack or series of attacks is not limited to a geographical area or a company's reputation, but can ruin entire industries as well as upset the stability of a nation. Furthermore, an organization may be unaware that it is the victim of a severe cyber-attack until it is too late. Extreme weather and most terrorist events, however, are visible from the outset.

A Cyber First AID plan offers an effective path forward. With the right investment, the integration of IT and non-IT entities can ensure situational awareness and business continuity.

Alternative risk management strategies include the Computer Security Incident Handling Guide by the National Institute for Standards and Technology (NIST) (Cichonski et al. 2012). The NIST incident response plan gives specifics on preparation; detection and analysis; containment, eradication, and recovery; post-incident activity, together with discussion on coordination (internal and external) and information sharing (Cichonski et al. 2012). The next step in cyber risk management is providing a holistic organizational approach to ensure that all

core elements are fully engaged rather than viewing cyber purely as the responsibility of IT professionals. Rehearsing a cyber crisis response strategy with a holistic approach enables organizations to improve resiliency and recovery to major cyber events, and modify plans where appropriate.

3 Adaptability

The broad array of cyber threats and vulnerabilities requires customizing incident plans to the operations of an organization with greater specificity than natural disasters. Incident plans must also be flexible to evolve as an event plays out. Unlike natural disasters with more predictable and familiar risk characteristics where a common preparedness and response framework can be applied, cyber-attacks are not only hard to predict, but may evolve to circumvent countermeasures. Homeland security practitioners refer to such perpetrators as "intelligent adversaries," where behaviors and attack strategies evolve to circumvent countermeasures and capitalize on target vulnerability to maximize their objectives (Ezell et al. 2010). Regardless of the preparations taken to respond to a cyber incident, a lack of flexibility and adaptability can quickly degrade even the best of response plans.

Cyber threats require organizations to first map their vulnerabilities and resulting consequences to understand what type of events they are most exposed and sensitive to. The consequences may include financial loss, reputation damage, and even harm caused to individuals from attacks on critical healthcare or infrastructure systems. A vulnerability assessment then informs a customized crisis preparedness and disaster management plan. The incident plan is then maintained as a living document as cyber risk characteristics evolve, depending on an organization's systems and working practices, and new attack strategies cyber adversaries employ.

Perception mapping software tools can be employed to capture employee understandings of "cyber hygiene" and crisis readiness, and identify potential capability gaps and vulnerabilities. The process helps build relationships across disciplines and foster trust among decision-makers. It is unrealistic to think that scenarios and exercises will identify all potential threats. However, they can test the robustness and resiliency of a system designed to deal with specific and unknown threats, while being flexible enough to respond to a variety of events. Scenario planning can help identify types of external threat environments an organization might face based on potential vulnerabilities of businesses practices, and longer range threats over the next few years. A risk assessment can get organizations to think ahead of the different strategies and their trade-offs to ensure appropriate action is taken.

4 Integration

Organizations need to integrate IT and non-IT entities to ensure sufficient situational awareness and business continuity. Clarity of roles and responsibilities is also critical, combined with an effective alert chain to deal with constant cyber threats. A robust understanding of the alert chain includes understanding the threshold level for IT to alert senior management, identifying decision triggers, and managing information overload in identifying the difference between noise and a credible threat to react appropriately. Overreacting to a cyber threat can be equally devastating as underreacting.

A systemic approach to IT security is required rather than limiting it predominantly to the domains of IT staff, the Chief Information Officer, and the Chief Information Security Officer, as such limitations can and will degrade an incident plan.

While the architectural framework and workings may be beyond the understanding of non-IT staff, all employees are required to have a clear understanding of reporting procedures, guidance compliance, and how they should respond during an IT crisis. Staff need to know from the outset their roles and responsibilities. With a near constant bombardment of cyber-attacks, most of which are known small-scale threats defendable by standard antivirus software, a clear and delineated process is required for decision thresholds and decision-making.

5 Deliberateness

Organizations must clearly articulate and test their strategies as part of a concerted preparedness, response, and recovery strategy. Procedures need to be clearly documented and communicated, and training sessions used to inform best practices. In addition, simulation exercises should be used to test and modify response strategies. Preparedness measures need to instill a "cyber-hygiene mentality" to prevent and/or mitigate the unleashing and spread of a cyber-attack from, for example, opening infected email links to lax password security processes. Cyber hygiene extends to an organization's supply chain and key stakeholders, and manufacturers across industries need to ensure that critical circuitry is not compromised during the manufacturing, supply, and maintenance phases.

Simulation exercises can serve as a highly effective experiential process to train employees and test the

robustness of the preparedness of an organization. Wargame simulations, when set up appropriately, are a powerful tool for rehearsing decisions by simulating the interactions of multiple actors in a safe environment. The experiential approach means participants who divided into teams can experience and understand firsthand in a hypothetical yet credible environment the intended and untended consequences of decisions made to assess the robustness of strategies (Sheppard and Crannell 2013).

Methods of rehearsing crisis cyber response include exercises with IT and non-IT staff, scenario planning, and documenting staff perceptions of preparedness, response, and recovery. After rehearsing a cyber crisis response strategy to evaluate an organization's cyber crisis readiness, plans must be modified where appropriate. Not unlike the regular use of earthquake and fire drills that serve to increase awareness and response, organizations should set aside time for their employees to run "cyber drills," making them a part of normal employee training.

6 Defining success

Mapping an organization's cyber readiness and gaps through decision mapping tools and simulations can capture organizational perceptions and document progress and develop successful cyber-defense strategies. Successes can be measured against maintaining strengths and addressing deficiencies across core business functions.

First, a Cyber First Aid Performance Scorecard, for example, can survey IT and non-IT personnel on the perceived *readiness* of employees for a cyber-attack. Key areas the score card should include are people, structure and process, information, and training. "Appendix 1" includes a sample employee survey.

Second, a software-based decision mapping process employed during a facilitated workshop with employees can map perceived areas of *vulnerability* to cyber-attacks and *probability* of occurrence. Figure 1 illustrates how an aggregated organizational core mission impact graph can look like to capture the potential severity of a cyber event (perception of mission impact) and the probability of one occurring (probability of occurrence). The decision mapping tool will have collated data on a number of hypothetical yet credible cyber-attack scenarios generated either by cyber security subject matter experts or from client workshop participants who create their own cyber event list.

The third step is to use wargame simulations to verify and test the organizational perceptions of core mission

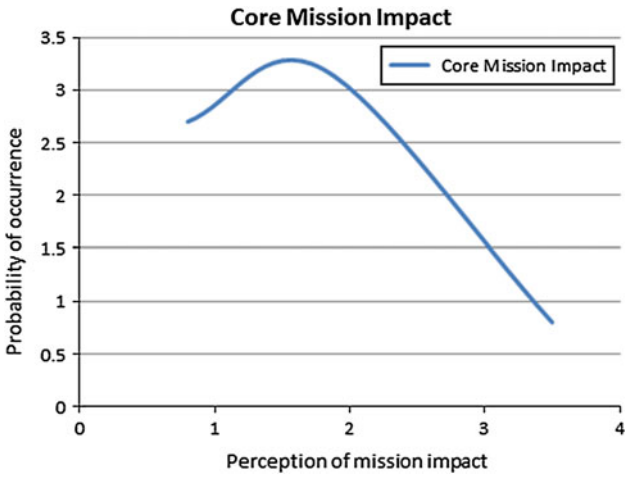

Fig. 1 Graph illustrates perceived higher probability of cyber-attacks, but a moderate impact on an organization

cyber preparedness and impact from cyber-attack(s). These can assess whether organizational perceptions are in line with actual cyber risks and response capabilities, and how these might differ across different groups, for example, IT and non-IT staff, by departments, and senior management versus middle management. Simulations can test the operating assumptions of the organization to expose potential vulnerabilities, gaps, and to rehearse staff in a "safe" decision-making environment.

Figure 2 illustrates how mapping the perceptions of staff before and after running a wargame simulation identifies gaps between the perceived and likely cyber risks and preparedness outcomes. The hypothetical graph indicates a shift in perception by staff on all four dimensions (probable impact, probability or occurrence, response capabilities, and organizational resilience) once staff have an opportunity to experience a cyber scenario. This example shows how the staff perceived a greater impact of a cyber event on the organization after the cyber simulation scenario exercise, a higher probability of occurrence, a less robust response, and less likely to rebound. This illustrates how wargame simulations can assist organizations to clarify vulnerabilities and focus on the areas that will ensure the most adaptable, agile response if a cyber-attack occurs. Mapping perceptions by itself is not a panacea approach, and some perceptions by employees may not be wholly accurate. Nevertheless, the approach greatly assists in identifying vulnerabilities and strengths to build a robust risk management plan. The perception tool could also be reviewed by cyber subject matter experts to provide their assessment of the perspectives and key outcomes.

Finally, the output from the simulations, perceptual mapping, and surveys can inform a cyber preparedness rubric that examines the competency of an organization's

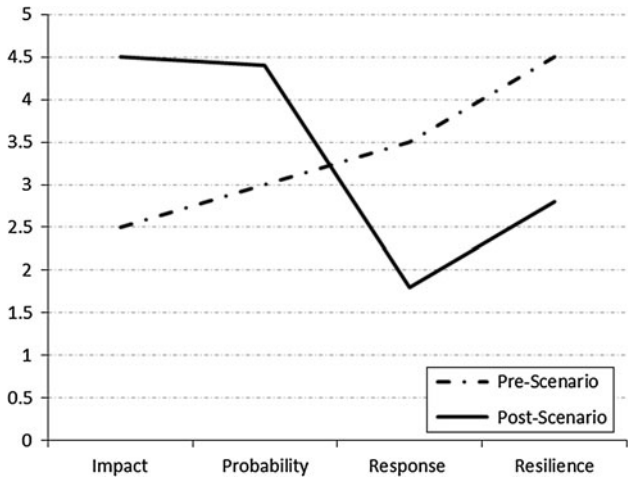

Fig. 2 Documented perceptions of staff pre- and post-cyber wargame

core functions. Each organization will naturally have a different set of internal and external mission critical core functions. Key questions addressed should include "what is at the core of the organization and what is most important to protect?" and "how best do you mitigate the risks and prepare for the second and third round of cyber-attacks?" In addition, it is important to think beyond the organization—"what partners and suppliers are critical to success?"—and "how will their lack of cyber hygiene hamper the organization's ability to respond?"

Internal functions include protecting confidential research and development data, and external functions include critical supply chain organizations that also need to review their own cyber processes. It is important that these functions are identified and for everyone within the organization to understand what those functions are and how best to protect them during a cyber-attack. The Cyber First Aid Preparedness table in "Appendix 2" illustrates what a rubric may look like. Across all core functions is a cyber preparedness rubric to assess the readiness, for example, whether mitigation strategies are documented, staffs are adequately trained to make timely decisions, and "workarounds" have been rehearsed to respond and rebound from a cyber-attack.

The cyber preparedness and contingency plans are designed to understand the decision trade-offs in a time of crisis. The more staff that understand the core functions of a business the better prepared they are likely to be in a crisis to make an informed decisions.

Shell Corporation, for example, attributes its speed of decision-making in a crisis to rehearsing the "what ifs" as illustrated by the company's agility to respond to the 1973 oil crisis after rehearsing a similar scenario. It is impossible to predict the full extent of a cyber-attack. But the more staff that participates in scenarios or cyber drills and think thru "workarounds" the better prepared the organization will be when the real attack occurs.

Cyber hygiene and adequate protective measures are a preferred approach to mitigate the consequences of cyber-attacks. We can expect these attacks to grow in intensity and frequency requiring effective Cyber First AID plans to meet the threat. The success of such plans can be measured in minimizing damage, maintaining stakeholder and customer satisfaction, and containing and eradicating the threat. Organizations can develop their own matrix of what they define as a success to their cyber responses, including recovery time, acceptable financial loss, and reputational damage. Given the pervasive and growing cyber threat and the need for organizations to be proactive and resilient, investing in appropriate preparedness, response, and recovery planning is the next logical step.

Appendix 1: IT first AID survey

Please take a moment to assess the IT readiness for cyber-attack

Evaluation Scale: (5) Completed; (4) Over 50 %complete; (3) In progress; (2) Just Started; (1) Not initiated.

People					
Initiative to foster team trust	5	4	3	2	1
Decision gym to build crisis decision capacity	5	4	3	2	1
Robust collaborative network to tackle robust collaborative network to tackle	5	4	3	2	1
Structure and process					
Integrated plan to maintain core business functions	5	4	3	2	1
Equipment to perform core functions	5	4	3	2	1
Back-up capacity to perform mission critical functions	5	4	3	2	1
Organization-wide information security policies and guidelines	5	4	3	2	1
Information and training					
Organization-wide strategy and plan to mitigate cyber-attack	5	4	3	2	1
Key IT management crisis decision roles defined	5	4	3	2	1

Appendix 2: Cyber First AID preparedness rubric

Each box can include a point evaluation and be accompanied by a short narrative description.

Evaluation Scale: (5) Completed; (4) Over 50 % complete; (3) In progress; (2) Just Started; (1) Not initiated.

Core functions	Engaged senior leadership	Documented mitigation strategies	Clarified decision sequence	Trained staff to make crisis decisions	Rehearsed workarounds	Instituted formal review process after cyber drills
Manufacture of product						
Delivery of product						
Customer information						
Financial information						
Talent information						
Confidential						
R&D information						

References

Cichonski P, Millar T, Grance T, Scarfone (2012, August) Computer security incident handling guide. National institute for standards and technology. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf. Accessed 26 Sept 2013

Curtis S (2013, July 29) Spy agencies ban Lenovo from secret networks. Telegraph. http://www.telegraph.co.uk/technology/news/10208578/Spy-agencies-ban-Lenovo-from-secret-networks.html. Accessed 19 June 2013

Ezell BC, Bennett SP, von Winterfeldt D, Sokolowski J, Collins A (2010) Probabilistic risk analysis and terrorism risk. Risk Anal 30(4):575–589

Heath T (2013) Living social is hacked, affecting 50 million worldwide. Washington Post. http://articles.washingtonpost.com/2013-04-26/business/38831562_1_cyberattack-zappos-customers. Accessed 26 Sept 2013

Potter N (2011, June 4) Sony hackers brag it was easy to compromise info from 1 million consumers. http://abcnews.go.com/Technology/sony-hackers-strike-claim-download-private-data-million/story?id=13753939. Accessed 24 Sept 2013

Rein, L (2013, July 13) At commerce dept., false alarm on cyber attack cost almost $3 million. Washington Post, p 6

Reuters (2012, December 9) Aramco says cyberattack was aimed at production. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0. Accessed 26 Sept 2013

Reuters (2013, July 5) Top defence and telecom firms join UK cyber security war. Telegraph. http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/10161463/Top-defence-and-telecom-firms-join-UK-cyber-security-war.html. Accessed 9 June 2013

Sheppard B, Crannell B (2013) The decision gym: decision insurance for organizations. Environ Syst Decis 33(1):138–151

Strategic Insurance and Risk Solutions (2011) Newsletter: from cybertedium to cyber attacks. http://www.strategic.net/documents/NewsletterNov2011CybertediumtoCyberAttacksFinal.pdf. Accessed 24 Sept 2013