Breaking down silos between business continuity and cyber security

Rick Phillips* and Brandon Tanner**

Received (in revised form): 1st October, 2018

*Stickley on Security, 4215 Miguel View Road, La Mesa, CA 91941, USA
E-mail: rick@stickleyonsecurity.com

**Rentsys Recovery Services, 23403 E. Mission Avenue, Suite 150, Liberty Lake, WA 99019, USA
E-mail: brandon.tanner@rentsys.com

Rick Phillips *has over two decades experience creating disaster recovery solutions and services for financial institutions in a highly-regulated environment. Rick partnered with Jim Stickley in 2014 to launch Stickley on Security to help companies prevent and address cyber security disasters such as data breaches and malware attacks through innovative education solutions to transition employees from a risk to a layer of security.*

Brandon Tanner *is a successful entrepreneur with a technology background that spans software, hardware and service solutions for financial institutions and other regulated industries. He is the senior manager for Rentsys Recovery Services, where he is the driving force behind the company's business continuity and disaster recovery products and services. The combination of Brandon's technology and regulatory expertise has led to several innovative cloud strategies that have helped customers maintain compliance more cost-effectively.*

Journal of Business Continuity
& Emergency Planning
Vol. 12, No. 3, pp. 224–232
© Henry Stewart Publications,
1749–9216

Abstract

Every year, most businesses experience a cyber attack of some sort. Despite the fact that these attacks can interrupt business operations, many organisations lack an effective business continuity response. While some organisations do have cyber security and incident response functions in place, they focus more on mitigating the attack itself than on ensuring business operations can continue in the interim. To understand why it is important to integrate cyber security into the business continuity plan, business continuity planners must first be familiar with the common cyber threats organisations face as well as the far-reaching impact of data breaches. Then, they must address the root causes of the breakdown between business continuity and cyber security: the lack of a security culture, boardroom support and a coordinated response. Practical steps for integrating cyber security into the business continuity response include starting a conversation with those responsible for cyber security, determining the appropriate response to cyber incidents, assessing the organisation's recovery needs and testing the response strategy. Ideally, however, organisations should prevent attacks altogether. As employees are often the primary point of failure in cyber security preparedness, organisations should improve their cyber security posture by investing in education and awareness from the top down.

Keywords: business continuity, cyber attacks, data breach, incident response, cyber security, education, awareness

INTRODUCTION

If 80 per cent of all organisations everywhere annually experienced a wildfire (or hurricane, or tornado, or flood), would business continuity planners make it a point to have a well thought-out response to that threat? The answer is yes. It is concerning, then, that many organisations lack a mature business continuity response plan to a threat that does affect 80 per cent of businesses in a single year: cyber attacks.[1]

Cyber threats have added a new layer to business continuity planning. Historically, business continuity planning focused on so-called smoking-hole scenarios, in which the business suffered a catastrophic disruption, such as a complete loss of a facility to a natural disaster. In other words, business continuity accounted for a worst-case scenario causing the inoperability of a facility, service or business function. Unlike disasters such as hurricanes, water-main breaks or widespread power outages, cyber threats are insidious. They have the ability to take down an entire operation, but customers — even employees — may not even be aware the threat exists until a function they use is impacted.

Within an organisation, cyber security and incident response strategies are designed to mitigate the impact of a cyber incident. These functions, however, focus on slowing the spread of an attack, restoring production systems and, if necessary, facilitating a data breach investigation. These processes are necessary, but the incident response plan typically does not account for how employees will continue doing their jobs if critical functions are impacted — and it should not. That is the purpose of the business continuity plan. The problem is that business continuity and cyber security are often siloed.

It is imperative that organisations develop coordinated business continuity and incident response plans to prepare for the rise of malicious threats.

GROWING THREATS

Examining the latest threats, the organisations they target and the risks they pose reveals why organisations can ill-afford not to incorporate cyber security into the business continuity plan.

Common threats

The full range of cyber threats is a topic in and of itself, but for the purposes of business continuity planning, the following are the most common types of attack vectors:

- *Phishing*: Phishing continues to be a mainstay of cyber criminals, whose methods are becoming more sophisticated, tricking even the most tech-savvy victims. Whereas phishing e-mails used to be fairly easy to spot due to poor-quality graphics and notoriously bad spelling, criminals are becoming better at mimicking well-known brands' e-mail communications. By harvesting data through social media, they are also skilled at whaling, or impersonating an executive for the purpose of tricking employees into divulging confidential information or wiring money.
- *Ransomware*: Ransomware is easily one of the most talked-about threats. Financial institutions, police departments, government agencies, hospitals and more have all been targets of this type of malware, which essentially holds a system or device hostage until the victim pays a specified amount of money — often in the cryptocurrency Bitcoin — to the perpetrator in exchange for the decryption key. Ransomware can be spread through e-mail attachments, infected programs and compromised websites. Security professionals recommend regularly backing up data so systems can be restored in the event of a ransomware attack. However, some strains, such as Cryptolocker, are now targeting backups.

- *Cryptojacking*: Cryptojacking is the use of someone else's compute power to mine cryptocurrency. Criminals execute the code by convincing the victims to click on a malicious link (typically in an e-mail or online advertisement) or visit an infected website. Once the code is downloaded, the only evidence is degraded computer performance. This attack strategy is growing in popularity because, unlike ransomware, it does not require criminals to wait for victims to pay a ransom, and they do not have to manage multiple decryption keys. Cryptomining is less expensive, and it generates more money for less effort.

Types of organisations targeted

Cyber security threats are not specific to any one industry sector or business size. For this reason, it is important that all organisations are aware of preventive measures and ways to combat an attack if it strikes. Enterprise organisations should also be prepared for the possibility of a cyber attack on the supply chain. Cyber criminals have been known to target small businesses as an inroad to larger organisations' networks.

Critical infrastructure is another popular target for cyber crime. In 2017, a hack triggered more than 150 emergency sirens around Dallas, TX.[2] A 2018 ransomware attack in Atlanta, GA, targeted several applications and devices within the city's government network, encrypting data and preventing customers from accessing city applications.[3] In Kiev, Ukraine, in 2016, hackers infiltrated a power supplier's IT network and manipulated supervisory control and data acquisition (SCADA) systems, causing a blackout in the capital city.[4]

It is safe to say that, at some point, every business will be affected by a cyber incident, whether as a result of a direct attack on the organisation's infrastructure or an attack on the supply chain or a public utility. With today's tightly-wound supply chains and customer demands for always-on service, failing to account for this risk can be detrimental.

The impact of data breaches

Not all cyber incidents lead to data breaches. When they do, however, the damages are far-reaching. According to Ponemon, the average cost of a breach is US$3.86m.[5] Verizon reports that 1,000 records breached results in total costs ranging from US$52,000 to US$87,000, while 10 million records breached results in total costs ranging from US$2.1m to US$5.2m.[6] While researchers have different methods of calculating the average cost of a data breach, it is clear that breaches have the potential for severe financial impact.

The long-lasting effects of a breach include competitive disadvantage, lost customers and revenue, increased acquisition costs, individual or class-action lawsuits, regulatory fines and investigative costs. By integrating business continuity with cyber security, organisations can reduce the cost of a data breach by approximately US$7.10 per breached record.[7]

THE BREAKDOWN BETWEEN BUSINESS CONTINUITY AND CYBER SECURITY

Ideally, those responsible for business continuity and cyber security should work together to create cohesive plans. The reality, however, is much different. Below are the top reasons organisations fail to form a collaborative business continuity response to a cyber incident.

Lack of a security culture and boardroom support

Developing mature business processes requires support from the top down.

Business continuity and incident response teams will struggle to meet their objectives if they do not have adequate budget, employee accountability and business-wide process compliance.

Unfortunately, many organisations lack a security culture. Two-thirds of executives say they are resigned to suffering a security breach in the future.[8] In keeping with that mindset, approximately 50 per cent of executives say they do not have an employee security awareness training programme or an incident response process.[9]

To get support for building a security culture, business continuity planners can start by getting buy-in from different business units and build an effective case to present to management. They should emphasise the benefits of a strong security posture for each business unit. For example:

- *Public relations and marketing*: avoid decreased market share and brand damage;
- *Customer service*: reduce time spent fielding inquiries from customers who have had their data breached;
- *Accounting*: protect profits and avoid disclosure of confidential financial data;
- *Legal*: reduce risk of lawsuits and compliance-related audits;
- *Human resources*: protect employee data; and
- *Procurement*: preserve ability to process secure, efficient payments.

Despite the fact that 87 per cent of business continuity planners consider cyber security to be their top concern, they struggle to address this risk via an effective business continuity response.[10] This struggle can be partially attributed to the fact that a separate cyber security team is responsible for mitigating cyber threats. Often, the cyber security team does not freely share with business continuity planners the results of cyber risk assessments and the planned responses to these risks. Likewise, cyber security specialists are not always aware of the organisation's business continuity response.

At the surface, this lack of information sharing is merely a symptom of organisational compartmentalisation. Upon further examination, however, it becomes clear that there are personal factors at play. Cyber security specialists do not want their response to be slowed down by unnecessary steps or people getting involved. For fear that their budget will be diverted or their jobs deemed redundant, business continuity planners do not want the cyber team to insert itself too much in the business continuity planning process. Staff members from both disciplines may also be motivated by a sense of self-preservation — if the strategy they have created is found wanting, will they be blamed?

However, when a business is affected by a significant cyber security threat, it may require the activation of both the business continuity and cyber security teams. Without coordination, the effectiveness of both plans could be negatively impacted.

As an example, consider the 2017 WannaCry attack, which affected 34 per cent of the UK's National Health Service (NHS) trusts.[11] The NHS did have emergency, preparedness, resilience and response plans in place, with NHS England designated as the point of contact for incident management.

However, the plans lacked clear guidelines for how local trusts should respond in the event of a national attack such as WannaCry — nor had the plan been tested at a local level. As a result, there was widespread miscommunication, with some local organisations reporting disruption to various entities other than NHS England, such as the police. Other trusts were unsure how to report the incident, either because the ransomware had infected their systems or because they had shut down their e-mail systems as a precaution.

The need for an improved business continuity response is evident from the fact that during the incident, staff resorted to unofficial communication methods such as personal mobile devices. In addition, because diagnostic equipment had also been infected, preventing healthcare workers from accessing important information, 19,494 patient appointments were cancelled.[12] A report by the Department of Health & Social Care, NHS Improvement and NHS England acknowledged that there is evidence that some local health and care organisations need to implement business continuity arrangements to prevent delays in care.[13] The report called for cyber vulnerability assessments to help with developing targeted responses.

PRACTICAL STEPS FOR INTEGRATING BUSINESS CONTINUITY AND INCIDENT RESPONSE

While it is easy to discuss the need for integrating business continuity and incident response at a theoretical level, formulating a plan of action is more challenging. The following steps help build a strong foundation for cross-functional collaboration.

Start a conversation

The first step is simple: start a conversation with those responsible for cyber security. The owners of business continuity and cyber security need to be transparent with each other. In some cases, that means admitting current procedures are not working and being humble enough to acknowledge mistakes. Having a culture of security encourages honesty, as people will be more willing to disclose and troubleshoot problems knowing that they have leadership's support. By addressing process deficiencies sooner rather than later, the organisation could mitigate a major vulnerability down the road.

Determine the type of response required for cyber incidents

It is important to consider the types of cyber incidents that could disrupt or halt business operations. Such incidents could include the following:

- Ransomware;
- Phishing/whaling;
- Accidental disclosure of data;
- Insider threat;
- Data breach;
- Cyber-related supply chain interruption;
- Social media breach;
- Drive-by malware download from web surfing; and
- Honeypots.

The business continuity and incident response plans should include specific responses to and procedures for such events. Not all cyber security incidents should trigger the business continuity plan, so it is important to determine what types of events or conditions will. For example, it is not necessary to activate the business continuity plan in response to an e-mail phishing incident that does not cut off access to critical data or affect users' ability to perform their jobs or provide service to customers.

Cyber security incidents with a wider impact, such as ransomware attacks, will likely require a business continuity response as an attack would prevent access to data and therefore affect employees' ability to do their jobs.

When a business continuity response is required, organisations should determine how employees will continue operations in those scenarios. For example, they may need to revert temporarily to paper-based processes or relocate to an alternative facility.

It is also critical that protocol be established for post-incident follow-up and remediation. Management should be given a debriefing of the response as well as any revisions needed to the business continuity and incident response plans.

Assess recovery needs

It is important to determine the business's recovery needs and procure any necessary resources ahead of time. The business continuity team can determine what resources are necessary for critical employees to resume operations, while the IT security team can help ensure that the security controls for the organisation's backup sites and alternative communication networks match the production environment's controls. The latter step is important to ensure that the vulnerability that caused the incident is not reintroduced when backup systems are spun up.

Backup resources may be required for the following:

- mainframe;
- midrange;
- servers;
- network;
- end-user hardware;
- operations processing equipment;
- office equipment;
- software applications and utilities;
- telecommunications; and
- data files and vital records.

Test the response

Having integrated business continuity and incident response plans is one of the best possible ways to mitigate cyber attacks. However, a response strategy that is not regularly tested may lead to unexpected issues that emerge during high-pressure situations such as a ransomware attack. The WannaCry attack on the NHS is a prime example.

Testing helps establish achievable recovery time objectives to limit downtime for critical business operations. Furthermore, some organisations — especially those in the healthcare and financial industries — must adhere to regulations that require organisations and their service providers to protect sensitive data while maintaining a certain level of uptime. Some of the common downtime threats are communication issues or process-related bottlenecks.

Testing allows organisations to assess critical, often interdependent, operations — such as recovering data, moving employees to alternative workspaces and running critical applications on backup systems — that may need to be performed simultaneously. In addition, a trial run of the response strategy allows participants to clarify communication protocol and the roles of personnel during an incident. To work through the details of how the strategy plays out in a particular scenario, it is beneficial to start with a tabletop exercise before doing a functional test. While testing takes time and resources, it reduces the cost and risk associated with a cyber attack.

MINIMISING CYBER THREATS THROUGH EDUCATION AND AWARENESS

While an incident response plan is critical to any organisation, the goal should be never to have to use it. The problem is that many organisations focus on the wrong forms of risk remediation. When speaking about cyber security, executives often indicate that the organisation is increasing its cyber security budget to implement the latest and greatest cyber security tools for thwarting cyber criminals. This fact alone is not an issue, but the breakdown of how those funds are spent often leads to major deficiencies in the organisation's overall security posture.

One of the most common mistakes an organisation can make starts with the overall classification of its cyber security management programme. Generally, the chief security officer (CSO) — or in smaller organisations, the IT manager — is responsible for maintaining cyber security. Meanwhile, a separate education department is responsible for providing training to employees, executives and board members. While executives are signing off for increased budgets to secure the organisation, those funds tend to flow directly to the department headed up by the CSO or IT manager, and education budgets see minimal increase.

'Education' is a broad term that covers everything from basic company policies to on-the-job training. Cyber security awareness is somewhere in the middle. While organisations have begun to understand the need for education services like internal phishing testing, cyber education has changed little overall in the past ten years.

To understand why cyber education is so important, one needs look no further than the breaches that appear in the news each and every day. In reading story after story, one common thread appears time and again: an employee clicked a link in an e-mail; an employee opened an attachment in an e-mail; an employee was browsing online and connected to a malicious website; an employee installed a malicious application on their mobile device; an employee gave confidential information over the phone; and so on. This ever-growing list highlights the employee as the primary point of failure. While cyber security products may help reduce risk, the reality is that as long as there are humans making decisions, technology alone cannot eliminate risk.

Employees

The terms 'education' and 'awareness' are often tied together and treated as one and the same. However, for any organisation to truly address the risks associated with employees, organisations must treat these components separately.

Education refers to the overall understanding of general concepts. This information is often stagnant and can be provided as quarterly updates (eg understanding what phishing is, how it works, how criminals can target employees, and ultimately how employees can avoid falling victim to attacks). On the other hand, awareness training must be a continual programme designed to keep employees up to date on the latest tools and techniques cyber criminals are using against organisations. For example, a new form of malware delivers an e-mail asking users to open an attached Excel spreadsheet and confirm that the numbers in the file are correct.

Awareness training is typically more specific than education and, in many cases, timely. The idea is that when an employee is aware of a specific form of attack, they are far less likely to fall victim. Therefore, by providing quick daily updates, employees not only become aware of the latest forms of attack but also continue to think about cyber security as a never-ending process.

One of the biggest mistakes an organisation can make is to implement a phishing training programme and believe they have addressed education and awareness. While phishing tests are important, the programme itself only covers one small area of education. Without implementing a more comprehensive education and awareness programme, many organisations actually mistake low failure rates on phishing tests as a sign of well-educated employees. It is more likely that employees, over time, learn how to detect the test phishing e-mails due to common threads between them. This does little to ensure employees will not fall victim to other forms of spear phishing, malicious websites or whatever new malware of the day is spreading across the internet.

Executives and the board

Members of the executive team and even board members are no less vulnerable. In fact, they are often targeted more than average employees simply because of the access privileges these individuals have. For example, a board member of a Fortune 500 company may have access to confidential documents that could impact future Wall Street earnings. In other cases, an executive may have access to personnel records containing names, Social Security numbers and other personally identifiable information. Despite the fact that executives and board members need education and awareness as much as employees do, organisations commonly exclude leadership from additional cyber security education.

Education basics

Ultimately, what goes into an organisation's education programme depends on the type of business an organisation conducts, the size of the business and the confidential information it maintains. That said, the following three activities should always be part of any education platform:

- provide general cyber security education quarterly;
- provide daily cyber security awareness updates; and
- conduct routine phishing testing.

Obviously, a robust cyber security education programme will require additional budget. However, if organisations are truly trying to reduce their cyber security risk, a small shift in budget dollars from IT to education can make a drastic impact on an organisation's overall cyber security posture.

CONCLUSION

Malicious cyber threats will continue to grow and evolve at a rapid pace. Organisations of all sizes and in all industries will be targeted sooner or later. To mitigate the full impact of cyber attacks, it is imperative for business continuity planners to engage the incident response team and formulate coordinated business continuity and incident response strategies. In addition, those responsible for cyber security budgets should allocate adequate funding for cyber security education and awareness geared toward employees, executives and board members. By developing cyber-aware employees, organisations may even be able to avoid attacks altogether. Considering the far-reaching costs of data breaches and reputation damage, these are steps organisations cannot afford *not* to take.

References

(1) Malwarebytes (2016) 'Understanding the depth of the global malware problem', available at: https://go.malwarebytes.com/OstermanRansomwareSurvey.html (accessed 29th November, 2018).

(2) CBS DFW (2017) 'City officials: Hack caused 156 emergency sirens to go off in Dallas', available at: https://dfw.cbslocal.com/2017/04/08/city-officials-hack-caused-156-emergency-sirens-to-go-off-in-dallas (accessed 29th November, 2018).

(3) City of Atlanta, Mayor's Office of Communications (2018) 'City of Atlanta launches online information-hub for updates on operations and the cyberattack', available at: https://www.atlantaga.gov/Home/Components/News/News/11530/672 (accessed 29th November, 2018).

(4) Polityuk, P., Vukmanovic, O. and Jewkes, S. (2017) 'Ukraine's power outage was a cyber attack: Ukrenergo', available at: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA?il=0 (accessed 29th November, 2018).

(5) Ponemon Institute (2018) '2018 Cost of a Data Breach Study: Global Overview', available at: https://www.ibm.com/security/data-breach (accessed 29th November, 2018).

(6) Verizon (2015) '2015 Data Breach Investigations Report', available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf (accessed 29th November, 2018).

(7) Ponemon Institute (May 2015) '2015 Cost of Data Breach Study: Global Analysis', available at: https://securityintelligence.com/cost-of-a-data-breach-2015 (accessed 29th November, 2018).

(8) NTT Com Security (2016) 'Risk: Value', available at: https://insight.nttsecurity.com/post/102d5th/riskvalue-report-2016-cybersecurity-risk-is-now-hitting-the-radar-of-key-busin (accessed 29th November, 2018).

(9) PricewaterhouseCoopers (2017) 'Global State of Information Security® Survey 2018', available at: https://www.pwc.ru/en/publications/global-information-security-survey-2018.html (accessed 29th November, 2018).

(10) DRI International (2017) 'New survey names cybersecurity, terrorism top business continuity threats', available at: https://drive.drii.org/2017/04/21/new-survey-names-cybersecurity-terrorism-top-business-continuity-threats (accessed 29th November, 2018).

(11) National Audit Office (2018) 'Investigation: WannaCry cyber attack and the NHS', available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs (accessed 29th November, 2018).

(12) *Ibid.*

(13) Smart, W. (2018) 'Lessons learned review of the WannaCry ransomware cyber attack', available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (accessed 29th November, 2018).