Business continuity planning and disaster recovery

The Sony Pictures hack should motivate organizations to prepare for the worst with business continuity and disaster recovery plans.

ebook

An SC Magazine publication

Sponsored by

Business continuity

Disaster can hit your organization at any time. But, there are strategies to help get formal security plans and policies in place to best serve your enterprise when, during and after a data breach strikes. Larry Jaffee reports.

Hollywood is fond of periodically reaching back to the past. But it was far from likely that its creative geniuses could ever conjure a disaster picture like the one that wreaked havoc at Sony Pictures this past Thanksgiving.

Hackers rendered the studio's computers and telecommunications inoperable and plundered its servers of everything: emails of top executives trash-talking its stars, health and financial personally identifiable information and salaries of past and present employees, even completed movies that hadn't yet been released. Adding insult to injury, the entire library of hacked Sony emails and documents is now available on WikiLeaks.

About a week after the massive data breach became public, the studio jerry-rigged a communications system that harkened back to a pre-internet/cellphone era.

"We are stuck in 1992 over here," an employee told *TechCrunch.com*. "We had barely working email [which didn't allow attachments] and no voicemail. Some people had to send faxes. They were dragging old printers out of storage to cut checks."

Sony Pictures CEO Michael Lynton admitted to the *Wall Street Journal*, "It took me 24 or 36 hours to fully understand this was not something we were going to be able to recover from in the next week or two." Indeed, for at least the next month, to get their work done Sony employees reportedly used their own mobile phones, Gmail accounts and iPads, as well as studio-issued BlackBerries (recovered from storage).

If anything, the Sony Pictures hack should serve as a wakeup call for all organizations to consider the importance of business continuity (BC) and disaster recovery (DR) plans However, an informal survey undertaken by *SC Magazine* of IT security professionals and crisis communications experts reveals that anyone could be caught with their pants down.

"Most organizations think about BC in some form or another, but few take the extra leap to commit to a robust and effective BC/DR plan," says Stephen Fried, an independent security consultant.

"It takes a lot of work, time and money to really ensure you can recover your operations in a timely fashion, and most organizations aren't willing or able to commit that type of resource," says Fried, former CISO of People's United Bank in Bridgeport, Conn. Simply taking backups of systems and data isn't enough, but unfortunately that's where the BC plan of many organizations stops, he adds.

Larry Bickner, principal manager of security programs for Verizon in Charlotte, N.C., agrees. "Businesses running close to their profitability are not interested in preparing for something that will probably take them out of business, oddly enough," he says.

Further, James Haggerty, CEO of New York-based CrisisResponsePro, a crisis management software tool that allows coordinated communication among all relevant parties, relays a recent incident: "A CEO of a large company says to me, 'Why should we plan for something that may not happen?'"

Haggerty says that companies of all sizes, from smaller businesses to Fortune 100s, "seem to want to turn a blind eye to crisis response issues, including business continuity in the event of disaster."

Fried notes a data breach is only one scenario why a business continuity plan should be ready to be put into action at a moment's notice when an attack rears its ugly head.

"A good BC plan covers a wide range of potential scenarios," says Fried. "Certainly, data breach discussions are all the rage right now,

$252M

in gross breach-related expenses since Dec. 2013, Target reported to the SEC.

so they are a good entry point to start the BC conversation if it hasn't started already." Once you have everyone's attention to the breach conversation, good security and business managers can leverage that attention to start developing a BC/DR plan that suits a variety of business needs, not just breach protection/recovery, he says.

But before that can happen, people must understand the different terminologies. Raj Samani, the London-based vice president and CTO, EMEA for McAfee, part of Intel Security, draws a degree of separation between DR and BC. "Disaster recovery is what you do immediately following something happening, whereas business continuity is what occurs after that event and allows you to continue your business in the longer term," says Samani.

Is preparation for an eventual data breach part of the same BC/DR discussion? That's a matter of opinion. "Unfortunately, with all the press, they are less and less the same conversation," admits Verizon's Bickner, pointing out that more businesses fail due to emergencies and disasters than due to data breaches, statistically. "CISOs have to go with what is trendy, and BCP is not these days."

Of course, well-run companies consider the risk management repercussions of its operations, but it's always a matter of corporate priorities and board oversight. Bickner's best-case planning scenario involves various financial and operational risks thoroughly considered by business owners.

"As security and BCP folks, we often follow a cookbook approach to BCP that leaves out the business except for raw inputs and review of final outputs," Bickner says. More often, the most forward-thinking business owners typically "discuss and argue their way to the best solutions due to their greater insight as to the sensitivities and interdependencies of their business," he says.

But he too draws a distinction between BC and DR. "Business continuity plans should take over where emergency/disaster plans end. It's a hand-off from emergency operations to recovery operations," he explains. BCPs should get more strategic, in his opinion, whereas emergency/disaster plans should focus on the tactics and procedures for dealing with an organization's probable top 10 emergencies.

Fried notes a robust crisis plan, as well as preparation for a breach event, will cover multiple scenarios, including system or facility failure. "A lot will depend on the organization's definition of 'crisis' and how all-encompassing the crisis planning effort wants to be," he adds.

OUR EXPERTS: Continuity

Ali Basit, assistant vice president, IT risk and compliance, QBE Insurance
Alan Berman, president & CEO, Disaster Recovery Institute (DRI International)
Larry Bickner, principal manager, security programs, Verizon
Stephen Fried, independent security consultant
James Haggerty, president and CEO, CrisisResponsePro
Reuven Harrison, co-founder & CTO, Tufin
Ondrej Krehel, founder and CTO, LIFARS
Larry Ponemon, chairman, Ponemon Institute
Raj Samani, VP and CTO, McAfee/Intel Security
Davia Temin, CEO, Temin and Company

Goodbye silos?

Corporate lines blur when it comes to cybersecurity matters – with risk management, crisis management, business continuity and disaster recovery often intersecting.

"They're really resilience people," explains Larry Ponemon, president and CEO of the Ponemon Institute, a research center based in Michigan. He says these are the folks who attend to bad things that happen, noting that the resilience team is focused on more than an IT security breach, but also other emergen-

$35M

estimated damage caused by the cyberattack against Sony Pictures Entertainment.

cies, such as a natural disaster or a fire.

A corporate culture bent on protecting turf within each silo, depending on function, may not be looking at the big picture (i.e., the entire enterprise). Ponemon advocates getting rid of silos, a major takeaway of the institute's 2015 cost of breach study. Silos, he explains, are dangerous because everyone is afraid of losing control.

Alan Berman, president and CEO of New York-based Disaster Recovery Institute (DRI), agrees that silos are disappearing. What's driving that trend? Simply the high-profile data breaches of the past 18 months.

Although cybercrime is often the catalyst when organizations seek help from DRI to prepare for and/or recover from disasters, the nonprofit typically borrows from business continuity lessons learned from natural disasters, for example, or other mishaps that interrupt operations.

An IT department, Ponemon points out, "may understand the technical stuff, but not understand the organizational ramifications as well. They tend to want to control things. You don't see that in other parts of the company to that extent."

Meanwhile, everyone within the organization must understand their well-defined role and where it fits within the business continuity management team, whose members all should be on the same page regarding "what is meant by resilience."

Education and coordination of the entire organization should start with senior management, including the CEO. "If you start from the top, you kind of create an atmosphere where being ready is a good thing," says Ponemon, thus better preparing the various business units to deal with rare events that could be potentially devastating. "No one wants to think about problems like, 'If we weren't attacked yet, I don't want to start thinking about the future.'"

Davia Temin, CEO of Temin & Co., a New York-based crisis management firm, agrees: "A cyber breach can be an extinction-level event for an organization if it's handled wrong or unfolds at breakneck speed unaddressed. That could destroy the organization."

During a crisis, a company's various stakeholders must be considered, she points out, posing basic questions: "If you're a financial firm, how does trading continue? How do you communicate with your customers? How are your people using email? Do they have access to email?"

If a call center gets hit with a tornado or hurricane, a company obviously must have contingency plans to outsource to a third-party vendor and backup data off-site. "That's the nitty-gritty, tactical operational stuff that makes businesses work," Temin says. That kind of planning should be going on all the time.

Ignorance isn't bliss

Forward-thinking organizations which make risk management an essential part of making their business strong have a tendency to readiness, and respond effectively to all sorts

Checklists: Business continuity plan

For further reference, you could check out these valuable resources:

ISO 22301 & ISO 27031 requirements for business continuity management systems: *www.iso.org/iso/catalogue_detail?csnumber=50038*

Citrix white paper: "Guidelines for Maintaining Business Continuity for Your Organization": *http://tinyurl.com/ossffmq*

AT&T's Business Continuity Planning Checklist: *http://tinyurl.com/bqmpj5q*

$3.8M

average cost of a data breach.

– Ponemon Institute, "Cost of Data Breach Study: Global Analysis," May 2015

of problems, including security exploits, says Ponemon. On the opposite end of the spectrum is the short-sighted, or "ignorance is bliss," mentality, which is convinced everything is okay because they are not aware of any major security vulnerability or threat. The problem with that thinking is that the organization might be unaware it's been attacked, and they falsely conclude everything is okay, Ponemon points out.

> "Somebody has to tell the CEO that there's bad news."
>
> *– Larry Ponemon, chairman, Ponemon Institute*

If BC/DR planning starts too low in the organization, what ends up happening is there is not as much buy-in, he notes. Managers may put together a narrow plan, but it's not customized to address specific circumstances that could happen throughout the organization. Even CIOs typically may not have enough clout to get the required resources.

Temin notes that many organizations – even those in the same industry – define differently the various aspects of recovery: risk management, crisis management, business continuity and disaster recovery.

"Despite what it's called, it's all part of the same picture," Temin says. They all come under 'risk,' he says, and should all report to an audit committee.

Ponemon recently studied an organization that had two groups focused on business continuity, risk assessment and IT incident response. One had hired professional services firm Ernst & Young. "They stepped on each other's toes," he says. "They were doing the same project twice. It was crazy and so inefficient."

Those kinds of things happen because there's not a good organizational structure of the BC people talking to the security ops people, he says. "It's hard for organizations to calibrate all of these different functions."

Shouldn't the various parties be talking on a regular basis? "Of course, they should," says Temin. In practice, do they? "No, not always." She views the recent ubiquitous wave of cyber breaches as the game-changer in enterprise risk management and business continuity that has captured the attention of boards. She works directly with boards, which are not only taking more of an interest when a crisis happens, they, in fact, are coming up with solutions to recover. They're coming up with a vision, assisting with coordination and making sure the systems are in place to protect its future.

"Boards demand accountability from a governance point of view and get on top of things when things are going wrong," Temin explains. Management is expected to come up with the right tactical, strategic plan to resolve crises.

A typical bottleneck could be communication. "It's a big problem when dealing with disasters," Ponemon says. "Somebody has to tell the CEO that there's bad news. The message becomes gobblygook. You don't want to put a filter on business continuity management because it could be devastating if the CEO is not aware of the issue."

Supply chain vulnerabilities

An organization's "risk appetite" and its exposures are based on various factors, including strategic, market, operational, compliance and reputational, notes Ali Basit, assistant vice president, IT risk and compliance for Irvine, Calif.-based QBE Insurance.

Exposure could come in the form of a weak link in the supply chain, as borne out by the recent massive hack – tied to two contractors doing background checks – of the Office of Personnel Management.

Similarly, Target Corp.'s computer systems were breached after its heating/ventilation/air conditioner vendor, based in Pennsylva-

23%

increase over 2013 in the average cost of a data breach.

– Ponemon Institute, "Cost of Data Breach Study: Global Analysis," May 2015

nia, was hacked. "[Target] ended up being a test case," DRI's Berman notes. "Credit card numbers ended up in Russia and Eastern Europe."

Indeed, supply chain issues have become so important to government regulators overseeing banking and health care, to name two industries, that banks and hospitals now tell suppliers to implement the same stringent systems they use "if you want to do business with us," Berman adds. Credit-card issuing banks, for example, have put into place the Payment Card Industry Data Security Standard (PCI) to help reduce credit-card fraud.

Organizations that don't abide by the guidelines leave themselves open to sizable fines, as well as class-action suits, as Target and Sony are now finding out. Target in April agreed to pay MasterCard-issuing banks as much as $19 million to compensate for losses related to the 2013 hack. The big-box retailer also settled a class-action lawsuit with customers for $10 million in March. Litigation against Sony related to its breach this past November is pending, although in June 2014 it agreed to pay $15 million related to when its PlayStation Network was compromised in 2011.

Berman notes that organizations can learn from an offline textbook case in avoiding a supply-chain breakdown, and how contingencies play an important role in preparing for the unwanted surprises. In 2000, a Philips plant in Arizona had a fire that left Ericsson without a semiconductor source for its mobile phones. As a result, Ericsson ultimately lost $400 million in sales, the beginning of the end for the company in that product category. Meanwhile, Nokia, which also received microchips from the Philips plant for its phones, had backup suppliers of microchips, and the fire didn't have as significant an impact on its operations.

At the time of the fire, Ericsson was a leading global provider of mobile phones. It sold what was left of that business outright to Sony in 2012 following a joint venture. In contrast, Nokia sold its handset business to Microsoft in 2014 for $7 billion.

From an IT security perspective, the best way for an organization to mitigate damage from malicious activity is to have a full backup of its data at all times, points out Reuven Harrison, co-founder and CTO of Tel Aviv, Israel-based Tufin, which streamlines the management of security policies for more 1,500 customers. "If anything happened to the original web server, you can very simply swap out to a replica server off the network," Harrison says. The replica – usually maintained by cloud-based, third-party vendors – is an effective means to prepare for an eventual attack and made availably by virtualization technology.

Where's your BIA?

IT security consultant Stephen Fried suggests organizations at a really high level implement the following best practices to assist in disaster recovery planning:

1. Develop a business impact analysis (BIA) for all critical systems. This will show the effect on the business if that system fails or is compromised.
2. Using those BIAs, categorize those systems in terms of the highest to lowest impact to determine which systems need to be recovered first and which can wait for a later time.
3. Work with the business leadership and IT to determine the resources needed to enact a "best-case" recovery scenario (or, more likely, multiple scenarios).
4. Deploy the technology and process changes that enable those recovery scenarios.

$154

average cost incurred for each lost record containing confidential information.

– Ponemon Institute, "Cost of Data Breach Study: Global Analysis," May 2015

He cautions that managing security across a replicated site, such as optimizing network policies to be fully in synch with DR architecture, is critical to be successful. "What could happen is you switch over to the disaster recovery site, and things won't work because your security policy is blocking them. Or your security policy is too open and people can get from the main site to the DR site, which will also allow an attacker to move between the sites."

> "It's one thing having something written down on paper..."
>
> – Raj Samani, VP and CTO, McAfee/Intel Security

Lessons learned

A major breach can and must prevent future problems, notes Ondrej Krehel, founder and CTO of LIFARS, a New York-based cybersecurity and digital forensic firm. "Companies adapt new response tactics once they learn hard lessons and review internal policies and procedures related to the user awareness section," Krehel says. Technical procedures and policies are often rewritten to reflect gaps, such as log retention, evidence preservation or monitoring.

Following containment of a compromise, LIFARS devises a remediation plan that sets up a systematic approach to plug security holes and provides short-, mid- and long-term goals in improving security maturity levels. A second part of the post-breach strategy focuses on the lessons learned and creation of a new security strategy for the enterprise that includes risk management provisions.

Further, a resilient organization periodically runs drills to see if its BC, DR and crisis plans actually work during a simulated event. Metrics include the time to respond and the estimated financial cost of resources to bring operations back fully.

During exercises, unforeseen issues not in the plan become obvious, notes McAfee's Samani, who asks rhetorically, "If there's a need for a backup generator, where does the diesel come from if there's a fuel strike?"

Staffs need to be not only made aware but also trained on what to do in time of emergency. "The resilient organization also should have utility," says Ponemon. "People need to understand the plan."

Samani agrees: "It's one thing having something written down on paper, but having teams to run through operations in which simulated disasters occur is critical because when a disaster occurs you haven't the time to sit down and download the document or try to read the policy about 'What do we do now?'" ■

For more information about ebooks from SC Magazine, *please contact Illena Armstrong, VP, editorial, at illena.armstrong@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, sales, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

$7.10

per compromised record saved having business continuity management involved in the remediation of the breach.

– Ponemon Institute, "Cost of Data Breach Study: Global Analysis," May 2015

Sponsor

HP is a leading provider of enterprise security solutions designed to mitigate risk and defend against today's most advanced threats. With market-leading products, services and innovative research, HP Enterprise Security Products enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense.

For more information, visit www.hpenterprisesecurity.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Krassi Varbanov
krassi.varbanov@haymarketmedia.com

SALES
VP, SALES David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

If you want better security, think like a bad guy.

Get to threats before they get to you. Today a global threat marketplace collaborates and innovates to attack our organizations 24/7. It's time to think like a bad guy. HP draws on decades of security experience to take the fight to adversaries before they attack. We can help you predict and disrupt threats so they don't become headlines—using insights from big data. And with HP Security Research, we are gathering and sharing intelligence to keep your business safe to innovate 24/7. Better security. See how it leads to a better enterprise. Visit **hp.com/go/security**