Exposed: Keeping Your Data to Yourself After an IT Breach

Mechanical Contractors Association MCAA of America

November 2014

Introduction

It happens every month: a Fortune 500 company releases a statement about a security breach.

"Our Data Center has been compromised."

"Credit card numbers may have been stolen."

"We are working with the FBI and will offer you credit monitoring services."

"We will harden our systems to prevent from future attacks."

Sound familiar?

It's the world we live in today. Cybersecurity and business continuity investments represent a meaningful percentage of a technology budget – and rightfully so, because while technology has made us very efficient, it also has made us extremely reliant on it for nearly every aspect of business operations. Many companies elect to invest dollars and time to prevent attacks and downtime. Others direct greater resources and attention to what to do once disaster occurs.

This white paper will navigate three common technology disasters facing corporate America today:

- a hacking attempt that hijacks company data for ransom;
- a website that is hacked and defaced; and
- a Data Center which goes completely offline with no estimate for restoration.

The purpose of this white paper is to educate MCAA executives on critical business continuity decision points and lessons learned by others faced with technology crises.

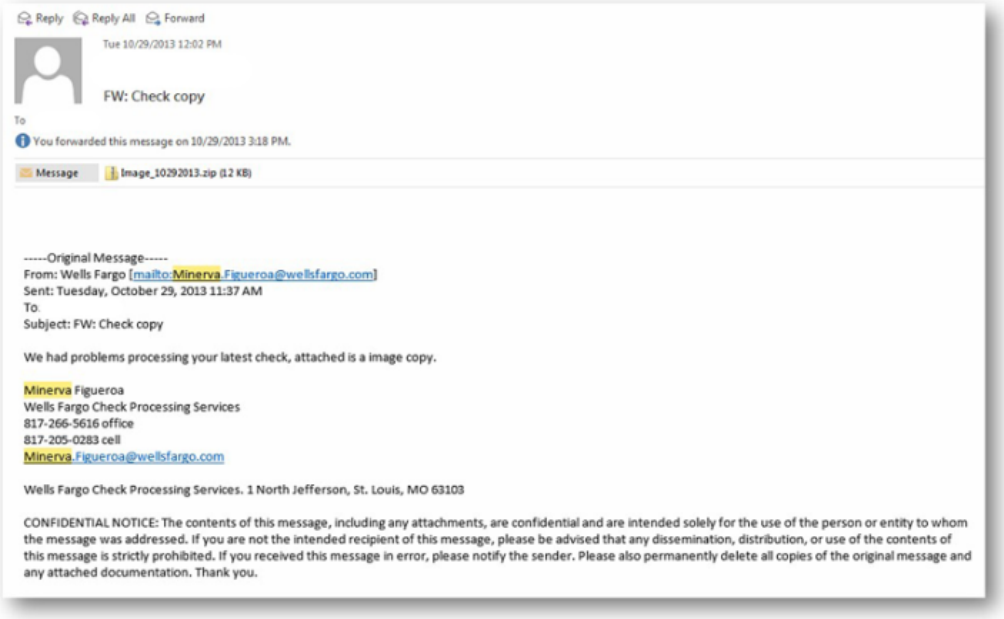
MCAA appreciates the work of our author, Matthew Ruck, Vice President of designDATA of Gaithersburg, MD, who has written a unique resource on a timely issue facing all of our companies. For more information, contact Lu Ann Steele Cornman at lsteele@mcaa.org.

Hijacked Data

How It Occurs

A new threat emerges in Corporate America: hijacked data held ransom by a new high-tech breed of pirate. The industry calls this "ransomware." While it sounds like science fiction, unfortunately it is not.

A little bit of history first… At the advent of the internet, malicious code traveled primarily by infected e-mail attachments – click to open, and a virus program was launched. As junk e-mail filters matured and began quarantining e-mails with attachments containing viruses, hackers began infecting websites, prompting users to download viruses without opening any specific file. Present-day hackers employ both of these tactics, sometimes in tandem. A typical scenario involves hackers blanketing large swaths of users with seemingly legitimate e-mail messages that have viruses as e-mail attachments or contain links to website-hosted viruses. You probably have seen examples. Common examples include e-mails claiming to be FedEx delivery receipts, banking messages, voicemail, E-Fax messages or outstanding invoices. The most prolific example of ransomware is the CryptoLocker Virus. See Figures 1 and 2 for examples.


Reply Reply All Forward

Tue 10/29/2013 12:02 PM

FW: Check copy

To

You forwarded this message on 10/29/2013 3:18 PM.

Message Image_10292013.zip (12 KB)

-----Original Message-----
From: Wells Fargo [mailto:Minerva.Figueroa@wellsfargo.com]
Sent: Tuesday, October 29, 2013 11:37 AM
To:
Subject: FW: Check copy

We had problems processing your latest check, attached is a image copy.

Minerva Figueroa
Wells Fargo Check Processing Services
817-266-5616 office
817-205-0283 cell
Minerva.Figueroa@wellsfargo.com

Wells Fargo Check Processing Services. 1 North Jefferson, St. Louis, MO 63103

CONFIDENTIAL NOTICE: The contents of this message, including any attachments, are confidential and are intended solely for the use of the person or entity to whom the message was addressed. If you are not the intended recipient of this message, please be advised that any dissemination, distribution, or use of the contents of this message is strictly prohibited. If you received this message in error, please notify the sender. Please also permanently delete all copies of the original message and any attached documentation. Thank you.

Figure 1
CryptoLocker: attachment-based distribution

-----Original Message-----
From: Incoming Fax [mailto:no-reply@efax.co.uk]
Sent: 29 May 2014 11:31
To:
Subject: INCOMING FAX REPORT : Remote ID: 486-448-6779

****
INCOMING FAX REPORT
****

Date/Time: Thu, 29 May 2014 16:01:06 +0530
Speed: 4138bps
Connection time: 01:05
Pages: 9
Resolution: Normal
Remote ID: 918-771-6137
Line number: 6
DTMF/DID:
Description: Internal report

We have uploaded fax report on dropbox, please use the following link to download your file:

https://www.dropbox.com/meta_dl/eyJzdWJfcGF0aCI6ICIiLCAidGVzdF9saW5rIjogZmFsc2UsICJzZX...
NmE2emFkbmlwMmYifQ/AAJkz3TpkNB7V2w0KL8LgZId9eoMyaOHI4NK9z6LtFZFYw?dl=1

****

Figure 2
CryptoLocker: link to virus payload

Taking Action

Once a user executes the CryptoLocker ransomware, either by opening an infected attachment or visiting a contagious website, the effects slowly begin to appear. As the virus spreads, it encrypts the user's files and they will no longer open. Depending on how much data there is, this process may take some time to occur, as the process of encrypting files is not immediate. The time needed for ransomware to perform file encryption is one of its primary weaknesses, and in many cases there is opportunity to capitalize upon this weakness to limit damage caused by the virus.

Action # 1: Train staff to report the issue immediately. The employee's timely notification to the IT Department is paramount in minimizing impact. The IT representative will disconnect the machine from the network.

Action #2: Determine if other parts of the network are infected. The IT Department will use tools to determine if the encryption has spread to other parts of the network. Interestingly, the effect of CryptoLocker as it spreads to network data shares is limited to the security rights of the infected user. If security rights to files and folders are tightly held and controlled, one department's security breach may not infect other parts of the company.

Action #3: Make an executive decision: are you going to pay? Once the virus has completed the encryption process on the infected machine, it will request payment by Bitcoin or another internet-based payment scheme to decrypt the files. Figure 3 below is an example of the CryptoLocker payment screen.

Figure 3
CryptoLocker payment screen

In 2014, the University of Kent performed a study on cybercrime victimization and reached a number of conclusions regarding the prevalence of ransomware infections and the resultant behavior from the victim. They found that 9.7% of the respondents reported a ransomware demand, and **more astounding is that around 41% decided to pay the ransom** (Hernandez, 2014).

So what did the other 59% do, and more importantly, faced with the same decision, what would you do? The following concluding actions outline the options you have.

Action #4: Confirm you have a good backup before the IT department removes the virus from your system. While this may seem contradictory or risky, if you remove the virus from the system, you lose the ability to pay the ransom. If you wish to keep this option open, proceed to Action #7.

Action #5: If you have a reliable backup, determine what the gap in time is between the last backup and the infection. This will determine, in terms of time, how much data will be missing once the data restoration completes. For example: if backup occurs at 1 a.m. every day, and the infection occurs at 4 p.m. the same day, after restoring you will lose nearly one business day of data. You should also ask IT staff if your server's built in ShadowCopy has any of the recent data you may be missing from the backup copy.

Action #6: Knowing that data will be missing, talk to staff to determine what work effort it would take to manually enter or recreate the data. It may be that the work effort is worth avoiding the ransom demands.

Action #7: If you decide to pay the ransom, know that you have a time limit to do so, and that the cost typically starts at several hundred dollars. It appears that the majority of users who paid the ransom were in fact able to restore the data. A caution: enter the code given by the ransomers correctly, as incorrect codes reportedly reduce the amount of time allowed by the pirates to comply with their demands. It reportedly takes three to four hours for the ransom payment to be verified, and the decryption process to occur (Abrams, 2014).

Website Defacement

Having your website changed by unauthorized parties is a frightening scenario for many reasons: it's highly visible, highly disruptive, and (unlike other disasters discussed here) it was led by a human's hand and was targeted at your organization.

Rouse the Troops, Stop the Bleeding

Once you identify that your website was altered, make sure you bring all of the right people to the table right away. A breach like this could have come from a variety of sources, and failing communicate as a group early on may slow your response time. At a minimum, include the teams that manage your corporate firewall, your servers, the website code, the website content, and any other databases or systems that are integrated with your web site, in addition to your website hosting company (if your site is hosted.) It may help to reassure all parties that no one's job is on the line because of a security failure, rather that you would like all teams to work together to help address this crisis.

The first action you should take once you have notified these parties is to shut down access to the website servers. This can include shutting off all access through the firewall, and may include isolating the Web servers from the rest of your network. You want to ensure that all unauthorized access is completely severed and that any back-door software that may be on your servers can't phone home. This will mean that your website will be completely down, but some down time is preferable to having the false or defacing information displayed. You may want to re-direct your entire website to an "Under Maintenance" page for the duration of the lockdown.

Where, What, and When

Once you have isolated affected systems, your technical teams will need to assess the damage. The modification of a simple HTML file on the website's home page is a very different scenario than someone changing records or tables in a back-end database or content management system. Ideally, your technical resources should determine where data was altered, including which systems, servers, or databases were touched, and identify which files or database entries were changed. You will need this information to formulate and implement a full response.

Determine How

This is the step that will require the most technical know-how from the task force you have assembled to address this issue. You will need to know how this unauthorized party gained access to your system to make these changes so you can ensure this won't happen again. The "how?" could be any number of things, including:

- The Web server allowed remote access from the outside world, and someone brute-forced the password.
- A database injection attack was caused by not fully sanitizing inputs from Web forms or poorly patched systems.
- The website fell victim to a known vulnerability from outdated search engines.
- An employee became disgruntled and intentionally caused damage.
- An employee was duped into installing malware from within the network.

You should also be on the lookout for other changes that may have been made throughout your systems during this penetration, including any software or system changes this unauthorized party may have installed that would give them unfettered access in the future. Such changes may be less obvious, and require extra attention to detect.

Your technical team needs to establish the "how?" and lock down the technology or procedure that allowed the unauthorized access, rather than simply undoing the changes or restoring from backup. Failing to address the root of such a system penetration leaves you with the same vulnerabilities that you had before.

Cleaning Up

Once you understand how the damage was done and have closed the vulnerabilities that allowed it to happen, you can focus on getting things back in order. If you have a backup of the systems from before the breach occurred, the most comprehensive way to recover is to restore from that backup, closing any vulnerabilities that may exist on the backup before restoration, then manually updating any code or content that may have changed since the backup was created. This may be a daunting task if a significant number of changes will be lost or will need to be re-entered. You may need to make a decision appropriate for your business that weighs the data loss versus the risk of not fully removing all possible traces and back-door access from the original breach.

Telling the World

Depending on the duration of the recovery, the duration and extent of the defacement, and the impact to your customers or members, you will very likely need to make some sort of announcement about what happened. You should consult with your public relations team and your legal counsel when formulating your response (especially if the incident caused you to miss some contract performance requirements or if there is a chance that customer data was altered, deleted, or copied.) Generally, you will want to be prompt and forthright in your statements.

While admitting that your organization is fallible is not ideal, having your customers or members doubt your honesty or integrity by delivering a late, incomplete statement or having none at all can be much more damaging to your reputation. It is important to be up front that an incident occurred, to

summarize the extent of what was impacted and for how long, and to emphasize that you've taken measures to ensure it won't happen again. Detailing technical minutia of such an incident is rarely necessary or desirable.

Investigating Who and Why

One of the hardest parts of this process to accept is that you may never know who took the effort to deface your website, or why they did what they did. If your systems were compromised by outdated software with known security holes, then any person with basic technical skills could have easily downloaded tools that would let them break in within 30 minutes. In this case, an attacker may have defaced your website just to see if they could, or for the same reason a teenager would spray-paint graffiti. Whether or not you engage law enforcement to investigate the breach is up to you, although it does not do any harm to report it. Jurisdiction on the Internet is a very tricky thing, especially if the breach originated from overseas, and tracking down the perpetrators often takes more resources than a small-to-medium-sized organization can reasonably spend. If you suspect that sensitive information was altered, deleted, or copied, then you should definitely engage your legal counsel.

Data Center Outage

Perhaps nothing is more frustrating than a server room or Data Center outage. Where do you start? A successful recovery from a Data Center outage is due to proactive work taken ahead of it.

Incident Response Plan

First, establish an **Incident Response Plan.** The plan will document who needs to be kept informed, their contact information, and the frequency at which updates will occur. Establish a standing conference call bridge and publish this to the plan. Denote important vendor relationships, support phone numbers, and account numbers. Remember that e-mail might not be working if your Data Center is down.

Part of your Incident Response Plan ought to include **basic network documentation.**

1. Network schematic/Visio diagram
2. Contact information for technology support team
3. List of servers by name, role, IP address, and physical / virtual location
4. Instructions for restoration
5. Prioritization schedule for restoration
6. Servers reboot sequence (servers often need to be turned on in a particular order)

Keep E-mail On

Many executives would tell you that e-mail now trumps the phone system as a business communication priority. Some are outsourcing or externally hosting technology functions with third parties to lessen

the impact of an outage. Many companies are **moving e-mail "to the cloud"** to retain communication functionality during outages. E-mail is a relatively simple function to move to the cloud, as most e-mail requirements are the same from company to company and do not require any specialized expertise. If you do not want to move e-mail to the cloud, consider utilizing a third-party junk e-mail filtering solution. Many of these solutions have extra features, such as virus scanning and filtering, message queues, message archival, and emergency inbox. **Message queues and emergency inbox services** are especially helpful in Data Center outages. These queues collect your inbound e-mail until e-mail services are restored, and prevent your clients from receiving bounce-back messages due to undelivered e-mails. Emergency e-mail boxes provide a website where you can send and receive e-mail messages while your e-mail server is under repair. See Figure 4 below for an example.

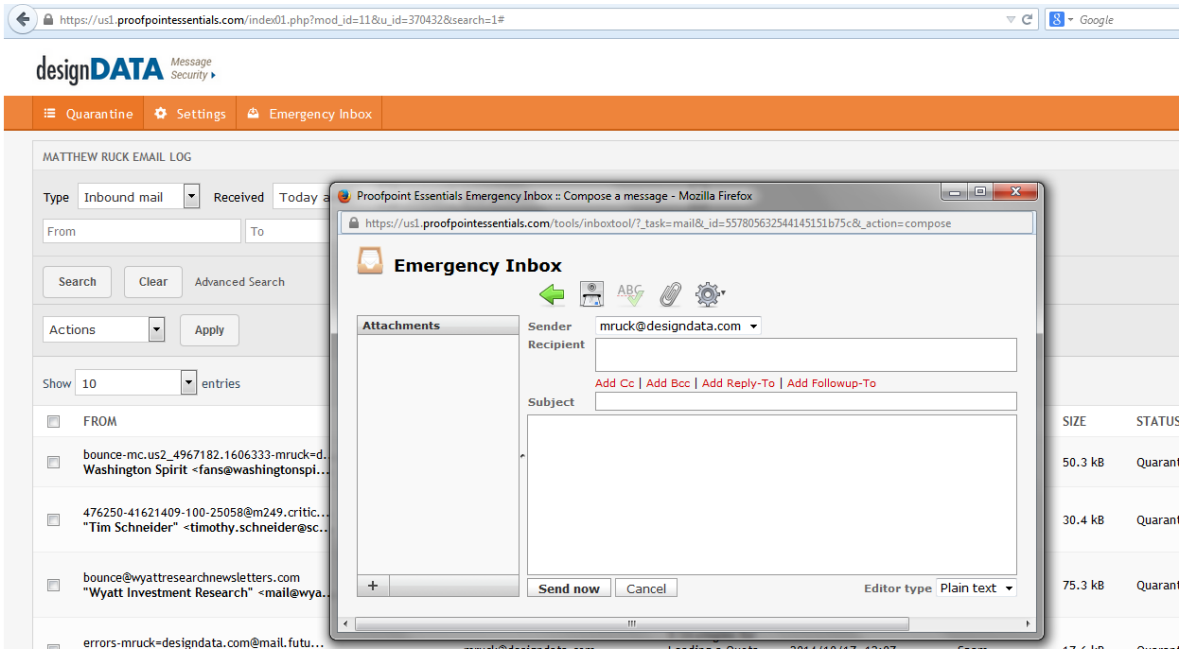


Figure 4
Example of emergency inbox services inside 3rd party junk e-mail filter (ProofPoint)

Virtualization simplifies

Virtualization of server infrastructure has revolutionized Data Center operations. Virtualization is a technology that allows multiple server instances to run on the same equipment concurrently. The same technology that collapses the servers virtually on fewer physical servers also greatly simplifies data backup and restoration.

Virtualized servers are portable to different kinds of hardware systems. This lends agility to disaster-recovery efforts; in the event of an emergency, the technology team has options and flexibility in procuring replacement systems. As a result, the time to restore is shortened substantially. In the past, server restoration was time consuming – a typically lengthy process requiring unreliable tape backup systems. Virtualized backups are comparably simple to run, administer, to recover from, and to replicate to another physical location.

Another frequently overlooked benefit of a virtualized backup is the ability to easily perform trial restorations. In the old days, performing trial restores or testing a system recovery plan was a herculean effort. With virtualization backup, images can be tested in minutes.

Failover Locations

The terms "hot site" and "warm site" are often thrown around as part of an IT risk mitigation strategy. "Hot sites" and "warm sites" are geographically separate locations, each containing servers and storage, with the backup site intended to be an on-demand, "flip the switch" replica of the primary location.

There are many reasons why this level of redundancy is not practical for the vast majority of businesses. First, it is very costly and requires high level technical expertise to implement this degree of replication and synchronization. Second, it requires ongoing maintenance and testing. Third, if you do failover to the backup site, it is often extremely difficult to fail back to the primary site. A good Data Center can achieve 99.9% uptime, which correlates to eight hours of downtime a year. Most companies can accept this level of risk vs. reward proposition.

Telecommuting Plan

Typically viewed as a benefit to keep talent, appeal to potential employees, and to save workspace, functional telecommuting plans are one of the most overlooked aspects of sound business continuity strategies. All contractors should evaluate what job functions should be able to continue under what circumstances when an office or site might be inaccessible and then discuss a regular telecommuting plan at the same time to understand the dual benefits of such a policy to the company. Offering remote connectivity to data and line-of-business applications to approved employees for remote work as a standard business practice means that these employees will also be comfortable working remotely in emergency situations, which will reduce productivity loss and panic.

For example, a mechanical contractor with two physical office locations and network infrastructure running in Data Centers outside of the workplace might operate a service division around the clock and require client-facing services (ticketing, phone system support line and monitoring tools) which must be operational twenty-four hours a day. In the event that offices are inaccessible, or in the event of inclement weather, staff could be instructed to work from home under certain secure conditions established by the company for the particular job function. Since all functions have already been evaluated for telecommuting and training and outfitting provided, employees have all the same tools they would use inside the offices when working from home unexpectedly, including telephony and important applications.

Bottom line: if you allow staff to occasionally work from home, when you need them to, they will know how.

Conclusion

When a technology crisis occurs, savvy and timely decision making is crucial to mitigating damage and downtime. While each situation may present unique variables, certain principles of technology management remain constant – namely, "An ounce of prevention is worth more than a pound of cure." It is the author's hope that diving into these three types of incidents provides a framework for your

company's response and aids you in moving the needle within your company to one that is well-positioned to handle any of these types of recently-emerging network technology crises.

Challenge your organization to answer questions that may have come out of your reading of this document. A useful exercise may be to consider some of the questions below:

- ☑ Have we trained our staff on security practices? Do they know not to click on suspicious links and attachments? Will they quickly notify IT if they notice a change on their systems?
- ☑ How does our backup work? Do we know how quickly we could recover (recovery time objective) and what our recovery points are (recovery point objective)? Have we performed trial restores? Are the backups performed with virtualization that would simplify and shorten the restoration time?
- ☑ Do we have adequate documentation? Would someone outside our top technical team members be able to use the documentation to aid in a crisis? Is the documentation up to date? Do we have a reboot sequence for server pre-requisites and contingencies?
- ☑ Is e-mail in-house? Is our e-mail junk filter in-house? Can we leverage a third-party junk e-mail filtering solution to either queue our e-mail, or, better yet, to provide an emergency e-mail inbox while our e-mail server is under repair?
- ☑ Have we created cost-effective strategies for business continuity, and have we provided the tools, training, and experience for staff to know how to compute and do their jobs from a remote location?

Works Cited

Abrams, L. (2014, August 6). *CryptoLocker Ransomware Information Guide and FAQ*. Retrieved October 16, 2014, from bleepingcomputer.com: http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#decrypt

Hernandez, D. J. (2014). *The Prevalence and Impact of Cybercrime Victimisation.* Canterbury, United Kingdom: University of Kent.

Mechanical Contractors Association of America
1385 Piccard Drive
Rockville, MD 20850
301-869-5800 • www.mcaa.org