KnowBe4
Human error. Conquered.

WHITEPAPER

Employees at the Frontline in the Battle Against Ransomware

Employees at the Frontline in the Battle Against Ransomware

By
Michael R. Overly, Esq., CISA, CISSP, COP, CIPP, ISSMP, CRISC*

As the recent noteworthy attacks in the healthcare industry have shown, no organization is safe from ransomware attacks and the results of those attacks can be devastating. By many reports, ransomware has been already responsible for causing hundreds of millions of dollars in damages, with no end in sight. Nearly fifty percent of victims have paid to recover access to their data. Nearly forty percent of those victims expect to be attacked again in the future. Given the ease with which ransomware can be propagated, the effectiveness of attacks, the untraceable ransom payments, and very low risk to the perpetrator of ever being brought to justice, we can expect a continuing rise in these types of attacks.

Organized crime, in particular, has become active in planning and propagating these attacks. Consider their risk-reward analysis. In committing a traditional crime, say a bank robbery, there is the inherent risk of physical injury, both to themselves and to bystanders, and, most importantly, the almost certain result of being identified and arrested. All that risk, for an upside, on average, of $10-30,000. In comparison, there is essentially no cost in initiating a ransomware attack, it can be sent from anywhere in the world (even in jurisdictions that have no laws against such attacks), it can easily be routed through servers world-wide to prevent the attack from being tracked back to its source, the attack has a high likelihood of success, and, best of all, the possibility of being apprehended is extremely low.

Businesses, particularly their officers and directors, have a duty to adopt procedures and policies and otherwise act prudently to address information security threats. Failure to do so, may give rise to legal and regulatory liability, loss of stock value, loss of revenue, and damage to business reputation.

> "The adage is true that the security systems have to win every time, the attacker only has to win once."
>
> - Dustin Dykes, CISSP
> Founder Wirefall Consulting

This is especially true when an attack such as ransomware can literally bring a business to its knees in a matter of minutes. As such, businesses must carefully plan to reduce the likelihood of ransomware attacks and to mitigate their effectiveness if an attack is successful. This means ensuring all antivirus software is fully updated and that disaster recovery/business continuity plans take the possibility of ransomware into account. Unfortunately, one of the most effective means of reducing the threat of ransomware is often overlooked: employee training and education.

To Disclose or Not to Disclose

Before turning to the training issue, there is one preliminary point that bears discussion. Specifically, under current law, is an organization required to disclose it has been the subject of a ransomware attack? The answer is not entirely black and white.

Most current laws and regulations requiring notification to consumers and, potentially, regulators relate to instances where there has been an unauthorized use or disclosure of protected information. The question is whether a particular attack results in such activity. In many instances, the hacker responsible for the attack may have access to the target's data. In such a case, the target of the attack would have a notification obligation. On the other hand, if the attack is of a kind where neither the target nor the attacker can access the data, there is something of a grey area.

In the healthcare context, a representative of the Department of Health and Human Services has said:

> *Under HIPAA, an impermissible use or disclosure of protected health information is presumed to be a breach (and therefore, notification is required) unless the entity demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment [various factors].*

As such, the healthcare provider must conduct an assessment to determine whether such a low probability exists. At least one member of Congress is contemplating whether the breach notification requirements under HIPAA need to be clarified or updated to reflect the ransomware threat.

Under other laws and regulations outside the healthcare industry, there are similar grey areas, but in many cases a ransomware attack may well require notification. We can likely expect further guidance on this issue from the courts and, more likely, as in the healthcare context, new proposed laws and regulations. Apart from breach notification laws, public companies should also consider whether a reporting obligation arises under the Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002 or other federal securities laws or regulations.

Employees at the Frontline

In many of the recent attacks, the initial entry point into the target organization has been attributed to employee error. Specifically, employees have clicked on attachments or hyperlinks in email or on web sites that provide the means of compromising their employer's systems. Ransomware and other exploits are becoming ever more sophisticated. While most employees hopefully know by now not to click on an offer from a Nigerian prince to transfer $20,000,000 into their bank account, many do not know the attacks may appear to come from their own banks or an airline with which they may have made a reservation. In each case, the emails may appear very genuine, including all relevant company logos and, even, references to their privacy policies.

In other cases, with a little effort by a hacker, an email can be further targeted using an employee's recent social media postings (e.g., the employee may have posted on Twitter that they recently dined at a local restaurant; a hacker could then spoof an email from that restaurant with the offer of a free meal).

Even highly sophisticated personnel can be taken in. Consider a simple example. A hacker decides to target the cardiologists at a large hospital. The hacker spends a few minutes trolling the hospital's web site for the names of all cardiologists; then spends another few minutes searching the web to find a nationally recognized cardiology researcher; next, the hacker inserts a piece of ransomware into a PDF file with the title "draft article"; finally, the hacker spoofs a message from the cardiology researcher to each of the hospital's cardiologists asking for their input on a draft article the researcher is working on. It is highly likely that one or more of the hospital's cardiologists will click on that PDF within a few hours, allowing the ransomware to insinuate itself into the hospital's systems.

Training is Key

While not a panacea, there is no question that proper employee education and training could avoid many ransomware attacks. It is on that point that this white paper focuses. It should be emphasized, however, that most training in this area amounts to little more than a handout provided to employees or, at best, a lunch-time presentation. The knowledge is quickly lost. To be effective, training and associated vigilance needs to be repeated periodically so that the information is truly internalized.

Employee education and training can have a twofold benefit: it helps to secure the employer's systems and also can have the side benefit of helping to better secure the employee's own personal computers and data. It is that twofold benefit that brings home to employees the importance of this training. We have found that employees are far more likely to have good security practices at work if they have good security practices at home and vice-versa. It is a win-win situation. Employees are more likely to take training to heart when they understand they are not only learning to protect their employer's systems, but also learning to protect their own most important home data (e.g., family pictures, videos, music, contact lists, important email, treasured documents, etc.).

Encouraging Personal Responsibility of Employees

Employees are the frontline of a business' information security defenses. While technological protections are essential (e.g., antivirus software, firewalls, spam filters, etc.), none are as effective as a vigilant end user. To that end, a checklist is provided below of measures of which every employee should be aware. By keeping these measures in mind, employees can dramatically increase not only the security of their employer's systems and data, but also their own personal computers and data. All too frequently, the security of one can impact the other. The goal is better security both at work and at home.

"You could spend a fortune purchasing technology and services, and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

- Kevin Mitnick

Conclusion

Ransomware poses and will continue to pose a substantial threat to businesses of every kind and size. No one is safe. To mitigate that threat, businesses must act to update their security procedures, policies, and protocols. Of course, this means ensuring appropriate technological tools are deployed, but, just as important, employee training and education must be provided. It is the synergy derived from the combination of technology and the human factor that will afford the most effective means of addressing this critical threat. If an attack occurs, determining whether there is a legal obligation to report the incident will turn on many factors. Competent legal counsel should be engaged to assist in determining whether a reporting obligation has arisen.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach. This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, vishing and smishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind. Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilized their end users as a first line of defense. For more information visit www.KnowBe4.com

---

*Michael R. Overly is a partner in the Information Technology and Outsourcing Group in the Los Angeles office of Foley & Lardner LLP. As an attorney and former electrical engineer, his practice focuses on counseling clients regarding technology transactions and information security. Mr. Overly has written dozens of articles and books on these subjects and is a frequent commentator in the national press (e.g., the New York Times, Chicago Tribune, Los Angeles Times, Wall Street Journal, ABCNEWS.com, CNN, and MSNBC). He has been asked to testify before Congress on privacy issues. His books on negotiating technology agreements, open source software, and big data have been recognized as "the" works on the subjects. Mr. Overly has conducted training for numerous US businesses, as well as those in Asia and Europe, on technology contracting and information security. Mr. Overly is one of the few practicing lawyers who has satisfied the rigorous requirements necessary to obtain the Certified Outsourcing Professional (COP), Certified Information System Auditor (CISA), Certified Information Systems Security Professional (CISSP), Information Systems Security Management Professional (ISSMP), Certified in Risk and Information Systems Controls (CRISC), and Certified Information Privacy Professional (CIPP) certifications.

KnowBe4
Human error. Conquered.

KnowBe4, Inc | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

Checklist for Employees

This checklist is intended to supplement, not replace, a business' formal security and information protection policies and procedures.

Web Sites, Social Media, and Public Email

- ☐ Don't get hooked on someone's fishing line. Do not reply to or click on links in emails, pop-ups, or websites that ask for personal information, financial information, health information. Never click on links or open files in an email from someone you do not know or weren't expecting.
- ☐ Always proceed with the understanding that no public email or messaging service (e.g., services provided by online services such as Google, Yahoo!, Microsoft, Skype, and others) is secure and that all communications will be stored and, potentially, viewed by others.
- ☐ Avoid sending highly sensitive information through unsecured email, texts, or other communications (e.g., Gmail, Yahoo mail, text apps on smartphones, etc.).
- ☐ Do not forward internal email, documents, or other information to a personal email address or download to personal devices for access outside of your employer's systems. Your employer cannot protect the information once it's been removed or shared outside of their systems.
- ☐ When submitting personal or other sensitive information via a website, make sure you see the site's address begins with https, as opposed to http. Think "s" stands for secure. Https uses encryption to send information across the internet, thus, reducing the risk that the information will be improperly accessed.
- ☐ Think before you submit. Once submitted to a web site or transmitted through an online communication service, the information is public. You never know where the information will show up. There is no such thing as deleting information from the internet. The internet is forever.
- ☐ Exercise caution using services and devices that record your communications (e.g., Google Voice, Siri, Cortana, Skype, VOIP applications, mobile app-based texting, etc.).
- ☐ Before posting pictures and videos online, remember they may contain GPS data showing where the picture was taken.
- ☐ Be mindful of backup applications running on personal devices (e.g., Dropbox, iCloud, Carbonite, etc.) making copies of sensitive company information and storing them online.
- ☐ Think before you open. If you don't know the sender, are unsure of why the attachment was sent, or if it looks suspicious, don't open the attachment. Better to verify with the sender then infect your computer, or worse, the network.
- ☐ PDF files are a very popular way of distributing viruses. Before opening a PDF, be sure you know where it came from.
- ☐ When installing apps on your smartphone be cautious of requests to access your calendar, contacts, texts, GPS, and other data. In many, if not most, instances, there is no reason for these apps to have access to your data and, in almost all instances, whatever you choose to share will likely be analyzed and sold to others.

Only Authorized Software

- ☐ Do not download or install unauthorized or unapproved software or applications from the internet.
- ☐ In particular, never install encryption software, remote access, backup or other similar software without the express approval of your information security personnel.
- ☐ Always be certain of the source of downloaded software (i.e., you are actually getting the software from the true creator of the software). It is common for hackers to create fake web sites and even "hijack" visitors from official web sites where applications can be downloaded. In some instances, the top search results for a piece of software on Google and other search engines point to disguised hacker web sites where your personal information may be stolen and viruses propagated.
- ☐ For your personal computers, make sure you have antivirus and firewall software installed. There are many inexpensive complete security packages available for home systems. Also, always promptly install security and other updates to your personal computer and mobile device operating systems.

Be Constantly Vigilant

- ☐ Be suspicious of calls from unrecognized numbers alleging to be security or other officials asking for confidential information, including account access credentials and passwords. Look up the person calling and call them back at their published number.
- ☐ Never reveal personal or business account access credentials or passwords in email or telephonically. No valid security personnel will ever ask you to reveal that information using either of these methods.
- ☐ Be wary of urgent requests to issue checks or take action to avoid some issue without confirming the source.
- ☐ Monitor the physical security of laptops, smartphones, and other mobile devices.
- ☐ Avoid using public internet Wi-Fi to access company systems without use of a secure virtual private network.
- ☐ If something is suspicious, report it.