The Return of Identity Theft: The Risk Fights Back

By Alison J. Cohen, Esq., and Guest Author David Kruse from Tetra Defense

When we last left off in 2019 "Identity Theft: The Rising Threat to Retirement," we raised concerns for service providers regarding fraudulent distribution requests and the rise of identity theft in the retirement industry. Since that time, there have been several prominent lawsuits in the news involving retirement plan participants who have been victimized by cybertheft and found no resolution with either the plan sponsor or the service provider (Estee Lauder, Abbott Labs, etc.). What is even sadder is our Firm's frequent involvement helping clients get through the worst experience of their lives, becoming the victim themselves of identity theft.

Identity thieves are getting more creative and sophisticated: implanting secret forwarding rules into the email box of its victim; using ransomware to hold entire databases hostage for bitcoin or other monetary compensation; and selling personal information on the dark net to be used to falsify distribution and loan forms.

Compounding these terrible events is the current environment in which we find ourselves. During the COVID pandemic, more people have been working from home, most likely on an insecure network, instead of through a secure VPN. More clients are sending data to their service providers through unsecure email, rather than secure portals, opening windows (pardon the pun) for more violations. Added to that is the post-COVID economic depression that has led to more desperate individuals turning to criminal activity.

Where's the white knight when we need one?

So, What's the Worst That Could Happen?

Assuming a cyber-attack exposes participant confidential information, the victim company is obligated under most laws to: (a) inform the participants of the attack; and (b) offer free credit monitoring to anyone who is concerned. A typical cyber-attack will likely cost at least $1.50 per affected participant just to do the initial mailing, additional costs for the credit monitoring (think $30 per person), and then actual costs if there is a theft incident. So, for a larger company with 10,000 participants, it is reasonable to assume potential costs in excess of $75,000. In addition, if actual theft occurs, it is likely that the plan sponsor and participant will want the company whose

computer system was invaded to “make good” any losses—particularly those that reach six or seven figures … or even more. (Even a smaller firm cannot only feel the financial pain, but the time, emotion, and stress-related toll this can take is devastating, not to mention the damage to client relations.)

Understanding the Transfer of Cyber Risk

Enter: your insurance broker. For all the criticisms the insurance industry receives (and, in some cases, may deserve) about being a complex, slow-to-change group of multi-national conglomerates, it’s proven to be very nimble in responding to the increased risk of cyber-attacks. And, having a properly written, well-understood, cyber insurance policy can be the difference between making it through an incident relatively unscathed or emerging at the end, significantly battered and bruised (or, frankly, perhaps not emerging at all).

One of the first well-known computer viruses was the Love Bug, a computer worm from early 2000, that corrupted files of the user who unwittingly clicked on a “love letter” sent via email from a stranger. Shortly after that, the very first cyber insurance policies were drafted, allowing businesses to recover their costs of dealing with attacks like this. As the decade continued, further innovation in cyber insurance resulted from businesses seeking financial stability in the face of increasing privacy regulations and the associated uncertain regulatory fines/penalties to which they could be subject after a data breach. During the decade following, starting in 2010, email scams/wire transfer fraud, credit card skimmers, and ransomware attacks continued to further impact businesses, often to the tune of hundreds of thousands of dollars (or more). This impact has encouraged the cyber insurance market to continue broadening its offerings to meet the increased risks facing businesses.

This rapid evolution in coverage prompts a few questions: Is any of this covered by my current insurance? What does cyber insurance actually do for me? How do I know if my broker knows my cyber risk?

Is any of this covered by my standard insurance?

Short answer: no. Unless you take affirmative action to secure coverage for cyber events, your existing coverage (property, general liability, director’s and officer’s liability, professional liability, etc.) very likely has exclusionary wording for cyber events written into the policy. Furthermore, if any coverage is offered, it’s likely a token amount that won’t satisfy your need. As noted above, simply the cost of the advisory mailing and credit monitoring can overrun the token sublimit included on your policy, if cyber coverage is included at all.

What does cyber insurance actually do for me?

Beyond providing coverage for “first party costs” (such as ransom payments, fraudulent wire transfers, incident response costs, and notification/credit monitoring costs for individuals whose private data was stolen) and “third party costs” (including legal defense, liability, and regulatory fines/penalties), a good cyber insurance policy will provide a framework for your incident response. This can include a breach coach (e.g., a privacy attorney) to quarterback your response; digital forensics specialists to diagnose the problem, negotiate ransom payments, and restore systems; crisis public relations teams; and more. Responding to a cyber-attack is not a do-it-yourself project.

How do I know if my broker knows cyber risk?

Ask your broker to detail what your most significant risks are, how they might impact you, and how a cyber insurance product will help transfer those risks. Ask about the current state of the cyber insurance market (coverage availability, pricing trends, etc.) and how many cyber insurance policies they've written previously. All of this will give you an idea of your broker's comfort level and actual experience.

Like any insurance product, you'll need to complete an application and be underwritten for coverage. Expect the carrier to ask about current security controls in place, types of data stored on your network, and past cyber-attacks you've experienced (if any). If they don't ask for any of this information, that is a sign that the policy might not be the appropriate one for you and you should pursue other avenues of coverage.

Steps You Can Take to Secure Your System

If insurance is the net behind home plate, risk management (and an appropriately mature information security program) is the catcher. A good understanding of the threats and risks to an organization is an important starting point to determine budget and specific controls to be implemented.

What are the most significant threats to an organization right now? Ransomware, wire transfer fraud, and business email compromise. These three threats account for the vast majority of cases that incident response firms work. The reason? They are wildly profitable for threat actors, and very difficult for law enforcement to prosecute. Most organizations, though, are not in a strong position to defend themselves from these attacks. Many companies trust their information technology ("IT") staff to handle information security. In reality though, information security should function as an audit to IT. The roles may be similar, but you could say bankers and accountants are similar, too; similar does not mean interchangeable. When IT is solely in charge of information security, it is common for software to be purchased that only addresses one issue, and then additional piecemeal purchases are required as new issues arise. The result is a system that is not well-integrated and, thus, much less effective.

Instead, by concentrating on these primary areas (at least initially; a mature information security program does much more than just what is described here), you can reduce the risk that your organization will fall victim to one, two, or all three threats noted above (as well as ones not discussed).

Multi-Factor Authentication

Multi-Factor Authentication (MFA) requires that users input a secondary piece of information (e.g., a code within a smartphone app/text message) into a system to gain access. Your organization should use MFA everywhere possible, but especially for remote access to an internal resource such as cloud-based software programs, remote access tools, and backup systems.

Aggressive patching and updating of all systems and services

Most attacks exploit issues for which there exists an available fix. Any security-related patch should be deployed as soon as possible. This includes servers, workstations, and network infrastructure, as well as services and applications installed on them.

Control and protect services exposed to the public Internet

Limit the services you expose to the Internet (e.g., web servers, email servers, file transfer mechanisms, or remote access services) to the very minimum necessary and isolate and segregate those systems from internal network and systems that are valuable. Ensure that any service that does face the Internet is "locked down" according to vendor and industry best practices.

Use advanced anti-malware tools

Your system should use advanced anti-malware tools instead of traditional signature-based antivirus protection. The former monitors systems, looking for patterns that might indicate a compromise has occurred; the latter simply looks for known code (the "signature"), which means that you can still be caught off-guard by code that's unknown to the program. It is also just as important to actively monitor the output/alerts from these tools. Getting warned is only helpful if you see and heed the warning.

Make information security awareness training a priority

It is useful to think of every employee of an organization as a human firewall—that is, an integral part of the information security program. Far from being a boring exercise, there is a lot of role-based training available that is organized, targeted, engaging, and interesting for all company employees. Proper training is an essential aspect of an information security program. Your employees need to know which seemingly benign actions are actually risky behaviors and what on-the-job signs of a security breach look like.

Less is (sometimes) more

A strong information security program does not necessarily require a huge investment in tools and software licenses. Often, the tools you need exist within software you already own; they simply need to be activated and configured properly. Avoid the fog of more.

Information Technology and Information Security

Information security very often is viewed as a roadblock, speedbump, or bottleneck for progress. For an information security program to be effective, you need advice from someone who is trained and experienced specifically in risk management and information security—someone who has the wider view of current threats, risks, compliance and regulatory obligations.

With strong collaboration between information security and information technology, a secure organization is often much more effective and efficient. A good example is asset management. If there is a single "pane of glass" that shows every computer and device, along with its hardware and software status, the information security team can see which machines are not running the latest (and most secure) versions of software, which are vulnerable to invasion, and the like. The IT team can use this tool to pre-emptively troubleshoot problems and errors—often before the users even notice that there is a problem—and commonly can fix the issue remotely and quickly.

Conclusions

People avoid dealing with subjects that aren't in their comfort zone, and computer issues are no exception. But, avoiding system security, and thinking that your current IT team has the

necessary expertise to combat the unseen threats that are out there, can be a lethal mistake. Have a discussion with your insurance carrier and make sure that you have the proper coverage, in case you get caught in the web of identity theft. Let the experts do what the experts do, find an information security vendor that can configure your system, secure reasonable and appropriate cyber insurance coverage, and sleep well at night.

FERENCZY
BENEFITS LAW CENTER
We are your ERISA solution™

Ilene Ferenczy • ilene@ferenczylaw.com | Alison Cohen • acohen@ferenczylaw.com
Adrienne Moore • amoore@ferenczylaw.com | Adriana Starr • astarr@ferenczylaw.com
Tia Thornton • tthornton@ferenczylaw.com | Leah Dean • ldean@ferenczylaw.com

2635 Century Parkway Suite 200, Atlanta, GA 30345
T 404.320.1100 | F 404.320.1105 | www.ferenczylaw.com