CAPINTECH

What We’ve Learned from Recent Cyber Breaches

By Allison Davis Ward, Partner

Organizations are plagued with cyber threats. There have been many high-profile breaches over the past few years, and unfortunately, the number of unreported breaches is likely much higher.

With incidents now a matter of *when*, not *if*, it’s important to understand the current trends in cyber breaches. Understanding the current threat landscape will help you encourage your teams and leadership to properly focus on and invest in cybersecurity and tighten your cyber defenses against the top risks.

Here are four key lessons from recent breaches.

Lesson 1: No industry is immune.

While privacy and breach notification laws continue to emerge, breach reporting is not currently a nationwide requirement. However, there are numerous resources that give insight into the state of breaches.

Organizations in the health care and financial sectors have stringent reporting requirements, and significant breaches are reported in the news. And various organizations perform annual studies on breaches and cyber threats, such as the annual IBM Cost of a Data Breach Report. The information from these sources highlights that **no industry is immune.**

Over the past 18 months, we have seen a large range of industries affected by cyberattacks, including retailers, secondary and post-secondary educational institutions, telecommunications companies, governmental agencies, cities and townships, police departments, fuel pipelines, social media companies, technology vendors, and marketing companies.

The key takeaway is that no organization should believe it’s not a potential target. All industries and organizations are at risk of a cyberattack and should establish cyber controls accordingly.

Lesson 2: Organizations without sensitive data can still be an ideal target for a cyberattack.

Designing controls to protect sensitive information is a significant component of cybersecurity. But several recent breaches have shown that cybersecurity isn't just about protecting sensitive data. It’s also about keeping your organization and systems operational. The high-profile cyberattacks at Colonial Pipeline Co., the largest fuel pipeline in the U.S., and meat producer JBS USA Holdings Inc. are perfect examples of this.

These two attacks resulted from ransomware. But the primary impact of each attack was not the exposure of sensitive data — it was the shutdown of critical operations. When testifying to the Senate Homeland Security Committee, Joseph Blount, the CEO of Colonial Pipeline, said, “I know how critical our pipeline is to the country, and I put the interests of the country first.” Similarly, JSB U.S. CEO Andre Nogueira told *The Wall Street Journal* that “It was very painful to pay the criminals, but we did the right thing for our customers.”

These statements indicate that both organizations felt they had a duty to their customers to restore operations quickly.

A lack of sensitive data does not prevent a cybersecurity attack. If your organization has operations that you want to keep functioning or a duty to provide crucial services to your constituents, you could be an ideal target for an attack because bad actors know you may be inclined to pay a ransom to become operational again.

Lesson 3: Your vendor supply chain presents risks.

In 2013, Target was one of the first big examples of a major breach resulting from a third-party relationship. More recently, the breaches at SolarWinds, Kaseya, and Accellion illustrate how impactful cybersecurity weaknesses in our vendor supply chain can be if the risks are not properly mitigated.

Several recent breaches have shown that cybersecurity isn’t just about protecting sensitive data. It’s also about keeping your organization and systems operational.

SolarWinds and Kaseya provide network management solutions used by individual organizations and managed service providers (MSPs) that manage client systems. In both instances, a vulnerability in the software was exploited by bad actors who then pushed out fraudulent software updates. Once installed, the updates allowed the bad actors to exploit the various systems.

Accellion provides file transfer software used by numerous industries — including higher education institutions, health facilities, financial institutions, and CPA firms. A security flaw in this software allowed bad actors to steal sensitive information, and several organizations found their constituent information on the dark web as a result.

Organizations rely on third parties for many functions. However, the oversight of these vendor relationships and responsibility for the associated risks remains with the organization.

Understanding the risks vendors can pose will help you develop proper due diligence for managing these relationships. This may include evaluating the vendor's security controls periodically, establishing procedures to promptly identify and apply patches released by the vendor, or configuring strong application controls on your systems.

Lesson 4: Old threats are here to stay, and they can lead to multiple levels of extortion.

The breaches in recent years have shown that we are still battling the same threats. Ransomware is not new, but it has continually evolved and is becoming increasingly layered. With ransomware, your data is encrypted and if you don't have backups, you may choose to pay the ransom. However, the impact doesn't stop there.

One example of a ransomware attack that led to multiple levels of extortion occurred with a Finnish psychotherapy clinic, Vastaamo. The clinic was breached starting in 2018 and experienced the immediate impact of ransomware. Then the attack resurfaced again in 2020. Patient data was exfiltrated through the attacks and the bad actors began targeting patients directly, requesting money in exchange for not releasing their personal information.

> Bad actors try to profit off a single attack as much as possible. They may extort you, your partners, your board, your clients, or other constituents.

Bad actors try to profit off a single attack as much as possible. They may extort you, your partners, your board, your clients, or other constituents.

Be aware that old threats like phishing and ransomware are here to stay, and your organization should continue to evolve your controls to effectively combat these changing threats.

What area above do you feel impacts your organization the most? Check out the additional resources below to learn more about these areas.

And contact us at cybersecurity@capincrouse.com with questions or to discuss how the CapinTech team can help you evaluate your organization's cybersecurity risk and provide meaningful recommendations to reduce it.

Additional Resources

- Ransomware article series: Understanding Ransomware: Malware in Its Cruelest Form, The Current State of Ransomware, and How to Take Your Ransomware Controls to the Next Level
- The Need for Vendor Management: Outsourcing the Support but Not the Oversight
- CapinTech Cyber Series Recorded Webcast: The Criticality of Vendor Management and Due Diligence
- Anatomy of a Phishing Attack
- How to Protect Your Organization from Phishing Email
- Cybersecurity Training: Who, What, When, Where, and Why

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA