Top Lessons Learned from Real-World Cyber Attacks

What You Can Take Away from the Cyber Attack Experiences of These Nonprofits and Professional Services Firms

B.F. SAUL INSURANCE

Expert Advisory. Claims Advocacy.

Over the past decade, the incidence of cybersecurity attacks has been escalating at an alarming rate, with Cybersecurity Ventures estimating the global cost of cybercrime to reach $8 trillion in 2023.

And it's not just the large, publicly traded corporations that are targeted. Nonprofits and professional services firms of all sizes are attractive targets to cybercriminals for a variety of reasons, making it critical for organizations in these sectors to be hyper vigilant.

Every cybersecurity incident offers valuable lessons from which other organizations can learn to effectively manage such incidents. With that goal in mind, this guide reviews real-world cyber attacks on several nonprofit organizations and professional services firms, how the incident impacted the business, and how those businesses responded to the cyber attacks. This guide provides insights and practical advice on how to reduce your organization's risk of a cybersecurity incident and avoid the high costs and other damaging consequences.

Why Cybercriminals Target Nonprofits & Professional Services

First, let's examine why nonprofit and professional services firms are attractive targets to cybercriminals.

Nonprofits tend to store data on donors (who may be perceived as prime financial targets) along with vulnerable or at-risk populations, such as children, the elderly, and low-income individuals and families. They often work with third-party vendors that may themselves be susceptible to a security breach. And often, nonprofits lack the financial resources to invest significantly in cybersecurity measures and may not even perceive themselves as prime targets.

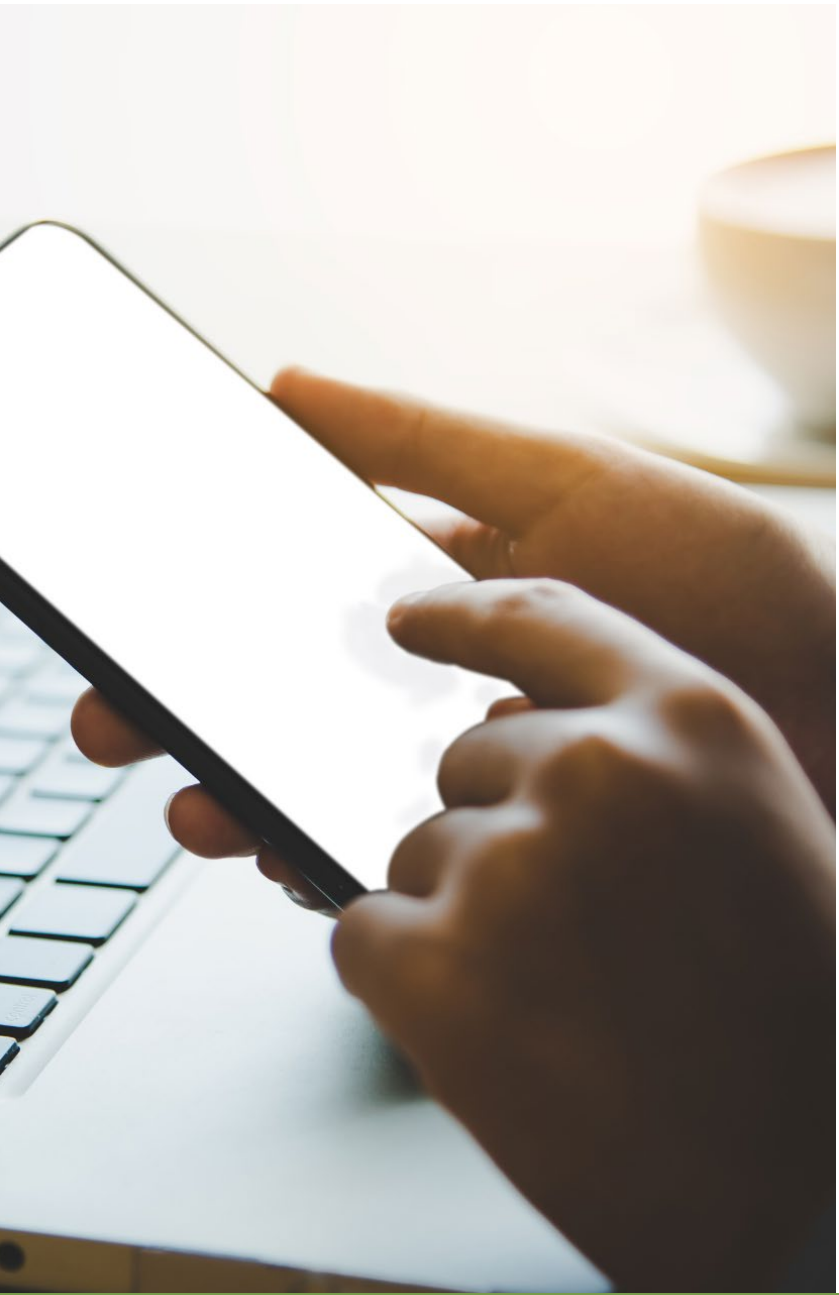
Professional services firms typically maintain sensitive, private, or confidential client data, so they are likely to pay to recover that data if it's locked by ransomware. Their employees often work remotely at client sites, requiring these firms to balance the need for access to documents, files, and data with the demand for security. Additionally, some lack the robust cybersecurity measures needed to thwart an attack or the disaster recovery plans and procedures to restore operations quickly and effectively.

As a result, for both nonprofits and professional services firms, the consequences of a cyber attack can be far-reaching and devastating. Aside from the financial loss, the organization might suffer reputational harm, lose clients or donors, face penalties and fines from regulators, or have to devote time away from the business to defend a liability lawsuit.

FIVE CASES

Five Different Experiences

Incidents like the following illustrate how easy it is for nonprofit organizations and professional services firms to fall prey to a cyber attack, along with the damaging consequences.



1. *The Red Cross*

Incident:

The Red Cross was the target of a sophisticated cyber attack on its servers that host personal data on more than 515,000 people. Per the organization's detailed FAQs, the hackers used tools that aren't widely available, along with techniques designed to hide and disguise their activities. The organization stated that the attack succeeded because it failed to apply an available security patch quickly enough.

Impact:

The Red Cross was required to provide notice to all impacted individuals whose personal information was potentially exposed due to the cyber attack. Based on the size of those individuals impacted, the notification process was described by the Red Cross as complex and ongoing, involving approaches like phone calls, hotlines, public announcements, letters, and even travel to remote areas to inform people in person.

Response:

The Red Cross relaunched its systems with the addition of several security enhancements, including two-factor authentication and advanced threat detection features.

2. *Philabundance*

Incident:

Philabundance, a large regional hunger relief group, was the victim of a social engineering scam, losing nearly $1 million when it paid what it thought was a legitimate construction bill for a new facility built for its Community Kitchen program. The $923,000 invoice actually originated from fraudsters who had infiltrated the organization's systems and sent a mimicked email impersonating an employee with what appeared to be a real invoice from the construction company on the project. However, the e-mail and invoice were both fake. It was only when the contractor inquired about the late payment that the organization realized it had been hacked.

Impact:

Philabundance stated that the incident didn't affect its day-to-day finances or its online donation system.

Response:

Philabundance enhanced its IT security systems and controls to safeguard the money it raises.

3. *Accenture*

Incident:

Accenture, a global consulting and technology firm, was hit by a cyber attack in which a ransomware group gained access to more than six terabytes of data. The attackers threatened to publish the information unless it received a ransom of $50 million.

Impact:

Initially, Accenture publicly stated that the incident had no impact on its operations. But months later, in a Securities & Exchange Commission (SEC) filing, Accenture reported that the attack did involve a data breach, that the criminals published some of the stolen data online, and that its clients "have experienced, and may in the future experience, breaches of systems and cloud-based services enabled by or provided by" the company.

Response:

The firm's security controls enabled it to identify the suspicious activity, isolate the affected servers, and restore those servers from their backups.

4. *Cadwalader, Wickersham & Taft*

Incident:
This global law firm experienced a cyber breach that placed more than 90,000 clients' personal information at risk and rendered many of its internal systems unavailable for weeks, according to some reports.

Response:
In notifying the affected parties, the law firm stated that it took steps to halt the breach as soon as it was discovered, reported the incident to regulators and law enforcement officials, and implemented measures to strengthen its network. The firm advised its clients to keep a close eye on their financial accounts and offered free identity theft protection services to those affected.

Impact:
A class action lawsuit was later filed, claiming the firm "failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach."

5. *A Large (Anonymous) Nonprofit*

Incident:
A nonprofit that provides financial advising services fell victim to a ransomware attack, with cybercriminals demanding $2 million to restore access to the affected files. Through a speedy response, the organization was able to contain the damage and negotiate the ransom down from $2 million to $500,000 and eventually to zero.

Response:
Under its recently purchased cyber insurance policy, the $1.2 million the firm had spent on forensic IT work, legal services, negotiation services, and proper notification was covered. Since the nonprofit had a history of strong service to its thousands of members, the organization avoided an avalanche of claims.

Impact:
Other than the lost manpower required to respond to the cyber attack, the non-profit was well positioned to deal with the breach through utilization of its cyber insurance.

INSIGHTS FROM
the Professionals

Brandon Newlands, Senior Vice President, Senior Director of Coverage and Claims, B. F. Saul Insurance, and David Katz, a shareholder with the law firm of Weissman Zucker Euster + Katz P.C., assessed these real-world cyber incidents to glean insights that other nonprofit organizations and professional services firms can learn from.

"In the nonprofit sector, organizations that experience a cyber attack often find their donors and other constituents, given the organization's larger mission and good works, will give them the benefit of the doubt [as to why the breach occurred]—the first time," Katz said.

"Generally, I think people understand that nonprofit dollars are focused on the charity's core mission and not necessarily data security. However, it is a major mistake for nonprofits not to focus on these risks. Most nonprofits must adhere to regulatory requirements for protecting private or confidential data, with stiff fines and penalties for noncompliance."

With or without regulatory requirements though, the court of public opinion is always a factor in the aftermath of a cyber incident. "The tolerance for mistakes might be higher for a nonprofit, especially a charitable organization, but any organization's members, donors, clients and other constituents will expect the organization to put the proper controls in place to avoid another cyber attack," Katz said.

Offering reparations also can help from a reputation standpoint. For example, the anonymous nonprofit referenced above offered every member a credit protection service for a period of time, which would have cost the organization in excess of $100,000 if it had not had robust cyber insurance.

While some organizations struggle to appreciate the full extent of their risk of a cyber incident, the available data is becoming harder to dispute. "There are many reputable sources that document the incidence of cybersecurity claims by company size and industry," Newlands noted. Providing those reports to senior leaders is a great first step toward increasing their awareness of the true level of risk.

Lessons Learned

Each of these cybersecurity incidents offers useful takeaways for any organization, especially nonprofits and professional services firms.

Size and Industry are Irrelevant to Criminals

A bad actor doesn't care if you employ a staff of 15 or 15,000. If they see financial opportunity, they'll target your business. And that's not just a function of the depth of your pockets; it's about the value of your data and its impact on your business. For example, a nonprofit's donor information can prove valuable to mine and sell, while a small accounting firm might find it difficult to be shut down for even a few days, making it a prime ransomware target.

A Cyber Response is Complex and Costly

Unless you've experienced one firsthand, it's difficult to fathom how multi-faceted, complicated, and expensive it is to respond to a cyber attack. Investigating the cause is just one important and costly piece of the puzzle. As these examples illustrate, a proper response also involves mitigating the damage, restoring access to files and data, and developing and implementing a notification plan. The notification requirements alone can be incredibly expensive to comply with, and the cost of a thorough response, including the forensic IT work and media experts to help mitigate reputational harm, could bankrupt a small company.

Cyber Insurance Is Just the Start

Despite the misconceptions, proper cyber insurance isn't just for companies in the tech sector. As case after case has shown, cyber coverage is essential for any business, especially a professional services firm or nonprofit. However, limiting your protection to insurance is a reactive approach.

In addition to budgeting for the proper coverage, it's prudent to allocate funds to proactive and preventive measures, such as assessing your system and network vulnerabilities and implementing stronger controls to fill gaps and address weaknesses.

The Insurance Requirements Are Not Trivial

Most cyber insurance carriers require the insured to have certain protective measures in place, which are becoming more stringent all the time. For instance, many require companies to use multi-factor authentication to verify identity. You'll find those requirements in the policy application, as well as the warranties section of the policy document. Some requirements may prove costly to comply with, but if you fail to meet the stated warranties and you experience a cyber incident, the carrier could deny coverage.

The Regulatory Requirements Vary

As of this writing, an estimated 13 states are requiring companies that fit certain criteria to assess how well they safeguard the data they gather, process, and store and to take steps to improve their controls where needed. More states are likely to follow suit in the coming years. In turn, carriers might begin requiring companies to guarantee they're meeting relevant state regulatory requirements for assessments and other measures.

The Notification Requirements Are Considerable

The detailed FAQs published on the Red Cross website serve as a prime example of a well-developed notification plan. The organization took a direct approach and used many channels to ensure it reached everyone who needed to know, even making in-person visits for people otherwise hard to reach. But consider how daunting the notification requirements can be for a nonprofit that serves tens of thousands of members or a mature services firm with 50 years of records. To ensure proper notification, It's helpful to work with an attorney who is experienced in advising businesses in the wake of a cyber incident. Most cyber insurance includes these legal costs as part of the coverage offered.

The Liability Risk Can Be Significant

"While a nonprofit's members aren't likely to bring a class action lawsuit after a cyber breach, that may not be the case with a professional services firm that serves clients," Newlands said. For legal and professional services, failure to safeguard data can trigger an errors and omissions (E&O) and/or directors and officers (D&O) lawsuit. Publicly traded companies are even more likely to see a class action lawsuit post-breach, especially if the incident negatively impacts the stock price.

It Pays to Develop a Response Plan Proactively

In the immediate aftermath of a cyber attack, emotions run high. That's why it's essential to develop a thorough, well-documented cyber response plan before trouble strikes. The ability to follow an established playbook can help your organization respond thoughtfully and strategically after a cyber incident. The very act of developing the plan helps an organization think through key issues, like what the chain of notification should be, how to comply with regulatory and carrier requirements, and which qualified vendors to call on for help.

Staying Cool Under Pressure is Vital

"When a cyber incident occurs, the immediate reaction is to panic," Newlands said. But it's important not to react emotionally or impulsively. "Knowing what to do and maintaining coolness under fire can make a big difference," Katz said, noting that a poor response can make matters worse by creating more exposure. Working with an attorney or an independent broker can help the organization to slow things down, think critically, and follow the incident response and communication plan the business has (hopefully) developed during less trying times.

Your Response is Only as Good as Your Third-Party Vendors

Given the highly technical nature of the cybersecurity field, it's vital to thoroughly vet and approve any vendors you choose to work with to investigate the cause of an attack and help restore data and operations. Be sure to drill down into any vendor's credentials and ensure you have complete trust in the experts you're counting on.

Ongoing Cyber Training is Essential

In the case of Philabundance, an employee's response to a fraudulent email opened the door to the breach. Companies are often shocked when this happens. But in reality, human error is the most common cause of cyber attacks, and that makes ongoing training and education essential. Many carriers will periodically test an insured's employees to see if they fall victim to a fake cyber attack attempt, then require anyone who fails the test to take additional training. With or without such a service, it's critical to make cybersecurity training a priority and allocate budget for it.

A Proper Post-Mortem Can Help

If your organization experiences a cyber attack, conducting a thorough post-mortem can help minimize the odds of future incidents. Bring together the key people to discuss what you could have done differently, where you need to make changes to address vulnerabilities, and whether you need outside resources to assist. It's easy to become fatigued after completing the initial cyber response and quickly revert back to business as usual, but it's essential to stay focused on preventing another attack or breach.

Turn to an Independent Broker like B. F. Saul Insurance

When it comes to protecting your organization against complex risks like cybersecurity, having an independent broker on your side can pay big dividends.

The financial lines specialists at B. F. Saul Insurance have helped countless organizations mitigate their cyber risk with proper insurance coverage and proactive risk management measures. We also stay on top of the ever-evolving cyber landscape to help you stay a step ahead of the risks.

To protect your organization against the growing threat of cyber incidents, schedule a call with the cybersecurity specialists at B. F Saul Insurance.

For legal advice and insightful best practices for risk assessments, incident response planning and responding to cyber attacks, contact David Katz at dkatz@wzlegal.com.

Brandon Newlands, JD
Senior Vice President,
Senior Director of Coverage & Claims

B. F. Saul Insurance
301.986.6312
brandon.newlands@bfsaul.com

David F. Katz, JD
Shareholder

Weismann Zucker Euster + Katz P.C.
404.390.2941
dkatz@wzlegal.com

B.F. SAUL
INSURANCE

Expert Advisory. Claims Advocacy.

301.986.6000
www.bfsaulinsurance.com

7501 Wisconsin Avenue, Suite 1500E |
Bethesda, MD 20814