How to Prevent Cybersecurity Disaster in 2019 (What 2018 Taught Us)

Devolutions

THIS ARTICLE WRITTEN BY LIMOR WAINSTEIN, TECHNICAL WRITER AND EDITOR, IS PART OF OUR GUEST BLOG SERIES.

PLEASE CONTACT US IF YOU WOULD LIKE TO BE FEATURED ON OUR BLOG.

Cyberattacks continue to increase in both frequency and sophistication. Nefarious parts of the web contain guides that teach people how to perform phishing attacks and ransomware attacks. Furthermore, individual hackers and criminal organizations understand exactly how lucrative a successful cyberattack can be.

Organizations know that if they want **to prevent cybersecurity disaster, outdated reactive security approaches no longer cut it**. Some organizations have established security operations centers, which are teams of skilled security professionals who focus on monitoring and analyzing security systems to protect against threats.

One of the best ways of protecting against cybersecurity disaster, however, is to learn from incidents that have targeted other organizations. Knowing the causes of these incidents can give you an idea of the methods favored by cybercriminals, helping prevent your organization from falling victim to a breach.

With this in mind, **let's take a look at some of the main 2018 cybersecurity breaches and see how they can teach you to improve your defense:**

MyFitnessPal

In early 2018, it was reported that Under Armor, the sports manufacturer and owner of the popular MyFitnessPal app, had been subject to **a data beach that compromised the information of 150 million users** of the app. The compromised information included email addresses, names, and hashed passwords.

Despite the breach, Under Armor's positive security practices provided a great lesson in how to mitigate the damage and reduce the likelihood of future breaches. While the app's first line of defense was breached, the use of encryption to hash passwords made it almost impossible for outsiders to access user accounts.

Furthermore, the company disclosed the breach within 48 hours of finding out about it and instructed affected users to change their passwords immediately. **The prompt response and solid second line of defense helped to minimize the impact** of what could have been a devastating breach.

Another key takeaway is that as apps continue to collect data on people via wearable fitness devices and the IoT, the value of information obtained during a breach increases. This goes a long way to explaining why organizations can expect the volume of cyberattacks to increase every year.

Marriott International

The most surprising thing about the 2018 Marriott breach was that **it showed evidence of a lackadaisical approach to cybersecurity by a multibillion-dollar company**. Cyber criminals were able to bypass Marriott's outdated security defenses with relative ease, compromising the information of 500 million of the hospitality chain's customers.

The lesson here is that **organizations need modern solutions to deal with modern cyber threats**. These types of solutions include security operations centers, threat intelligence tools, SIEM software, and web application firewalls.

Panera Bread

The 2018 breach at U.S. bakery chain Panera Bread was so shocking because of how long it took to mitigate. The sensitive information of millions of Panera customers was found by a security researcher to be available in plain text format via an API endpoint on the Panera website.

Ignoring for a moment the obvious negligence in exposing such information via an unauthenticated API endpoint, the real story is that the company was informed of the problem **8 months before they dealt with it**. The lesson here should be to listen to security researchers and respond promptly if they take time to inform your organization of a cybersecurity issue they've found.

SunTrust

The breach at American bank holding company SunTrust was a high-profile incident that resulted in a class action lawsuit. This breach was revealing in that it exemplified the dangers of insider threats. A SunTrust employee allegedly **stole the information of 150 million of the company's customers** with the intention of selling this information to criminal organizations.

The 2018 SunTrust breach highlighted how important it is to take steps to prevent insider threats. Enforce the principle of least privilege, log and monitor employee interactions with systems, and conduct regular security awareness training.

South East RHF

Healthcare is one of several industries in which the nature of information gathered by organizations within it is extremely sensitive. South East RHF is a Norwegian healthcare provider that was hit by a huge data breach in 2018. **Hackers accessed confidential health information of nearly 3 million people**, which accounts for over half of Norway's population.

The attack was complex in its execution, and it is unknown whether it was preventable. However, it's clear that due to the sensitive nature of information gathered in some industries, **cybercriminals are starting to target organizations in such industries with more complex and more frequent hacking attempts**. State-of-the-art security defenses are needed where extra sensitive information is involved.

Conclusion

Cyber threats are evolving all the time and becoming more frequent, but it's evident from the many events in 2018 that basic IT security failings still play a huge role in many of the most high-profile incidents.

Considering the high costs and damaged reputations associated with serious cybersecurity incidents, **it's vital to take steps to get the basics right with a prudent and well-enforced security policy.**