CYBERRISKS+LIABILITIES

September/October 2018

IN THIS ISSUE

hierl

Who's to Blame if a Security Breach Affects Your Organization?

If a security breach affects your organization, your main focus may be to solve the problem as quickly as you can, not point the finger in blame. But your customers want to know why it happened and who was responsible, even if the breach occurred because of their own lax security measures (e.g., sharing passwords or opening suspicious emails). In fact, a recent survey found that 70 percent of consumers expect businesses to take responsibility in the event of a data breach. But who within your organization should take the heat?

The CEO

If an organization doesn't budget enough for security solutions, the fault will likely be placed on whoever makes the financial decisions, stemming from the CEO. In fact, 29 percent of IT decision-makers who took part in a recent VMware survey thought that the CEO should be held responsible in the event of a large-scale data breach.

The CISO

If a data breach occurs even after your company adequately budgets for cyber security solutions, 21 percent of IT security professionals surveyed would still hold your CISO accountable in the event of a data breach.

IT Personnel

According to a 2014 report, 95 percent of cyber security incidents are due to human error. That's why personnel who manage IT security on a regular basis are easy targets for blame.

Other Employees

While accountability may start with the CEO and board of directors, everyone in your organization should take responsibility for cyber security. Even if you have the most modern cyber security technology, its return on investment will be nonexistent without full employee participation.

Increase in Attacks Against 911 Call Centers Highlight Need for New System

There have been 184 cyber attacks on public safety agencies and local governments since 2016, and 42 of those attacks targeted 911 call centers, according to cyber security firm SecuLore Solutions.

Over half of the attacks involved ransomware, in which hackers used a virus to control the emergency systems and hold them hostage for payment. Most of the remaining attacks were denial-of-service attacks, which involved a flood of fake calls that prevented call centers from addressing valid emergency calls.

Due to the vulnerabilities in the current 911 system and the fact that it doesn't address the ways people communicate in the modern world—such as through texts—the emergency response industry is encouraging state and local governments to adopt a system called Next Generation 911.

The Next Generation 911 system will have advanced security and be able to seamlessly move incoming calls to other centers when needed. The new system also gives callers the choice of calling from a phone line or sending data through approved telecommunications carriers and internet service providers.

Next Generation 911 is expensive, however, and governments have been slow to adopt it. Plus, its increased connectivity also opens new potential means of attack, according to industry experts. Sophisticated defense systems run by in-house cyber security teams will be vital as the emergency response industry adopts any new technology.

Acronyms All Businesses Need to Know

In the world of cyber security, it's easy to get overwhelmed with all of the acronyms industry experts throw around in everyday conversation, especially when the acronyms represent unfamiliar concepts. Nonetheless, it's important to become familiar with these terms and understand their general purpose.

Addresses Perimeter and Endpoint Security

IDPS: Intrusion Detection and Prevention System – An IDPS generally involves both an intrusion detection system (IDS) and an intrusion prevention system (IPS). The IDS component contains a database of known attack signatures, which it uses to detect and monitor incoming threats. The IPS component is able to respond to events detected by the IDS.

EDR: Endpoint Detection and Response – An EDR solution is intended to detect and respond to anomalies in any of your endpoints. Endpoints are any devices connected to your network, including servers, workstations and modems.

Addresses Users and Data They Access

UBA/UEBA: User Behavior Analytics – UBA solutions focus on user behavior and are an affordable way to detect, report and respond to changes made to your critical data.

DLP: Data Loss Prevention – DLP does the same as UBA in that they both keep track of sensitive data and ensure that it isn't lost or mishandled. Unlike UBA, however, DLP focuses on the data itself—not how users interact with it.

Keeps an Eye on a Broad Range of Sources

SIEM: Security Information and Event Management – SIEM and EDR work together to aggregate data from multiple sources, but unlike EDR—which only monitors endpoint abnormalities—SIEM solutions are able to monitor events from a broad range of sources. Those include your IDPS, firewalls, anti-virus software, end-user devices, servers, network traffic and operating system logs.

Hierl Insurance Inc.
325 Trowbridge Drive
Fond du Lac, WI 54937
920-921-5921
www.hierl.com