CISO ToGo
Technology Risk Consulting

THE VALUE OF A CYBER SECURITY PROFESSIONAL

Cybersecurity has become a household word, but while we hear about data breaches and phishing scams on a daily basis, what does it all mean to your organization? Well, it could mean the very survival of your business! Below are **SIX SOLID FACTS** that demonstrate the critical and urgent need for trained, experienced cybersecurity professionals.

1. THE COST OF CYBERCRIMES

By 2021, cybercrimes will cost $6 trillion per year worldwide. The cost of cybercrimes will double in the next five years, up from $3 trillion in 2015, according to a report published by Cybersecurity Ventures. This includes not only stolen money and ransom, but also the value of lost productivity and intellectual property, data theft, business disruption, reputational harm and more. Experienced cybersecurity professionals can help reduce this cost for their organizations by putting protections into place, firming up security policies and identifying vulnerabilities before attacks happen.

2. RANSOMWARE ATTACKS

Businesses experience ransomware attacks every 40 seconds. According to Kaspersky Lab, between January and September 2016, businesses experienced ransomware attacks once every 40 seconds, up from the previous rate of once every 2 minutes. Also in 2016, the number of daily ransomware attacks jumped 300 percent, from 1,000 per day in 2015 to 4,000 per day in 2016. And nearly one-fifth of hacking attacks included ransomware. As the threat of ransomware continues to increase, it's important for organizations to have cyber-incident response in place so they know what to do when it happens to them.

3. MALICIOUS EMAILS

1 in 131 emails is malicious. More than half of all emails are spam, according to Symantec's 2018 Internet Security Threat Report, and the amount of spam containing malware continues to increase. Today, malware has gone pro, with authors outsourcing spam campaigns to specialists, and the scale of these operations indicates profitability, which means they will likely continue, according to Symantec. Training staff to use caution with unknown emails can be the first line of defense in cybersecurity.

4. NETWORK VULNERABILITY

Attackers reside within a network for an average of 146 days before being detected. Although this number has dropped from the previous 200-day average, the fact that hackers can dwell undetected for almost five months should raise a red flag. Experienced cybersecurity professionals can not only identify and analyze anomalies on the network, but they can manage vulnerabilities before an attack occurs.

5. OPPORTUNITIES ABOUND

Unfilled cybersecurity jobs will reach 3.5 million by 2021. Not to mention that today, cybersecurity is everyone's responsibility, from the help desk to the CIO and even non-IT employees. But the number of jobs specifically in the field of cybersecurity will increase exponentially in the next five years. And Cybersecurity Ventures estimates that by 2021 every large company globally will have a chief information security officer (CISO) in seat, compared to the 65 percent that have one now and the 50 percent that did in 2016.

6. IOT DEVICE VULNERABILITY

An IoT device can be attacked in less than 2 minutes. By the end of 2017, the world had 8.4 billion connected devices, up 31 percent from 2016, according to a Gartner study. While consumers are driving the adoption of IoT devices, companies will spend an estimated $964 billion on IoT hardware this year. Cisco estimates that the number of IoT devices will be three times as high as the global population by 2021! But what do connected devices have to do with cybersecurity? Not all IoT devices are created equal when it comes to security – some are put on the market so quickly that they have vulnerabilities. And the consumers using these devices may not set them up securely … so, when they bring their own devices to work, it exposes their employer to cyber-threats. IT pros need to apply behavioral analytics to IoT devices in the same way they do to computers, servers and the network. Anything could be vulnerable.

THE BOTTOM LINE …

Having trained and experienced cybersecurity professionals on staff can reduce an organization's risk to cyber-crimes exponentially. And when, **not if**, the organization does get attacked, an experienced cybersecurity pro can mitigate the problem and help to get the business back up and running quickly and efficiently ... **and that's where CISO ToGo can help**! To find out more information, check out our services listed on our website (www.CISO-ToGo.com).