SAHOURI
INSURANCE

www.sahouri.com

Trending: CEOs Lose Sleep Over Cyber Risks

By now, hopefully every business is familiar with the concepts of email, text and phone call scams, multifactor authentication, and cyber monitoring. Those are cyber basics for any company that uses the internet. But hackers make a living out of breaking in and getting around network protections. And it's worrying CEOs.

Cyber risk has been one of company executives' top 3 concerns for years, but the will to secure networks, communications, financials and operational systems has been lacking. This has led to major failures at utility and shipping companies, as well as insurers, pharmacies, retailers and financial services providers. There is hardly any industry that hasn't been hit — and hit hard. Here are the main weaknesses, and what to do about them.

Problem 1. Passwords

Hackers prefer the easiest route into your business networks. That typically is through exploiting weak or stolen passwords. While everyone hates dealing with them, password updates and unique, long, random strings of characters are a basic line of defense, pruning the low-hanging fruit that cybercriminals crave.

While it may be convenient to reuse passwords across multiple sites, this provides easy access to business networks. When a password is compromised on one account, it can swiftly be applied to all other accounts held by the user. So,

for example, if your employee has a social media account that uses the same password as their email account for your company, you have a potential unlocked door.

The password warning has been repeated many times, but password insecurities remain the most exploited gateways for cybercriminals. According to the cybersecurity firm Trusona, more than 80 of cyber breaches stem from weak or stolen passwords. So what can your company do

Password solutions: Even though employees may be annoyed by it, you should require a long string (- characters) of mixed letters, numbers and symbols. Make sure your employees are not reusing their passwords on any other accounts, and require passwords to be changed frequently as often as once a month. ou may even want your information technology staff to change the passwords on their end and require users to authenticate themselves to renew access.

Trend: Some companies are moving toward biometrics to eliminate passwords on mission-critical systems. These are high-end, more expensive techniques, but they are becoming increasingly mainstreamed and, therefore, affordable. They include fingerprint, iris, facial and voice recognition. The drawback is loss of access if something happens to the unique user and the identifying asset is lost or compromised (for example, a burn, eye loss or death). If you go this route, make sure you have an administrative workaround.

Problem 2. Lost devices

In today's economy, company business is increasingly done via mobile devices, which creates multiple layers of security risk. The most common scenario is the loss or theft of a device. In these cases, the data on the device may be used to your company's detriment. Devices include both company-provided and personal hardware that accesses business systems.

Lost device solutions: Every company that permits mobile access to its systems should ensure that devices can be tracked, recovered and or rendered useless (bricked) if necessary. A clear policy should be instituted so employees understand that any hardware — even personal devices used to access company networks may be monitored, searched and manipulated to protect company assets.

Trend: Endpoint hygiene, a series of protocols that provide device-level security, is increasingly being pushed by information security experts. It includes undeletable tethering, which ties devices (endpoints) to a governing program and cannot be turned off by the endpoint user. It allows real-time monitoring of a device's location and activity and immediate action to lock the device, prevent unauthorized access, and maintain regulatory and security compliance.

Problem 3. Lost compromised data

Data is vulnerable to internet hackers, as well as low-tech snoops who tie into hotspots, Bluetooth or other open lines of access. Businesses can and do use prevention, such as firewalls, encryption and virtual private networks, but professional hackers can pick basic commercial locks pretty easily.

And, unfortunately, businesses frequently don't run software and firmware updates, leaving open doors for cybercriminals. Centralization of company data, whether on the cloud or an in-house server, is also problematic. ust one infiltration into that data store could take your company out of operation and cost large sums to remedy.

Lost data solutions: Make sure your IT team is regularly running software and firmware updates to keep your data protected. Proper cyber management can go a long way toward deterring cyberattacks on your business. Also consider replacing legacy hardware that can no longer support software updates. If hardware can't be updated, your company is playing Russian roulette with every sign-on. It may be an expensive measure, but it will save you in the long run.

Trend: Data fracturing or "decentralization" is a new way to prevent hacker access to the mother lode of your crucial business files and ensure recoverability. Basically, your company stores pieces of encrypted data on segregated computers (called nodes) across a global network. It's an adaptation of blockchain that restricts access via keys that you can tightly control and invalidate, if necessary (for example, if someone leaves your firm).

To illustrate, imagine you use a single cloud provider. If a hacker infiltrates, they can snake into all your files. With decentralized cloud storage, each node contains only pieces of your data set, and the interloper cannot do anything with those encrypted, partial assets. But you can because you have the keys for all the different nodes. This is a nascent technology, but some companies are already using and perfecting it.

Problem 4. Insurance

Cyber insurance was a relatively new commodity a decade ago. At the time, many insurers jumped into the market with products to pay out under different scenarios, such as a company's liability for damage caused by a cyber breach; forensic research into what caused a cyber failure; and paying for data recovery and ransom demands.

Now, after five or so years of big losses and evermore intensive cybercrime attempts, insurers are pulling back and cyber insurance is becoming more expensive and harder to get.

Insurance solutions: Companies really can't afford cyber losses on their own and must transfer some of that risk to insurers. The best way to qualify for good coverage is to have competent cybersecurity protocols in place. In fact, many insurers won't consider a company that doesn't take serious steps to protect its data and systems.

Trend: Putting cybersecurity in your business plan and naming an executive who owns the strategy are recommended courses of action for companies of all sizes. Even if your organization can't afford an in-house cybersecurity team, you should consider what you can afford to outsource. This will ensure cyber needs are budgeted for, cyber solutions are rewarded and cyber failures can be minimized.

Client Advocacy

(703) 883-0500
advocacy@sahouri.com

Sa ouri Insurance Agency
inancial Services Inc
8 00 reensboro Dr
STE 550
Mc ean, A 0
www.sahouri.com