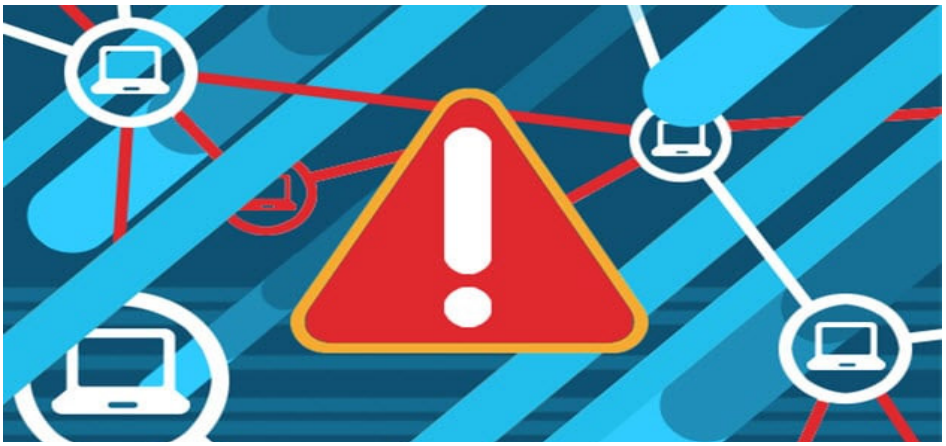
Talk Nerdy To Me

May 2022

7 Reasons You Need An Incident Response Plan



A strong incident response process can dramatically reduce the damage caused to an organization when disaster strikes. An incident response plan helps codify and distribute the incident response plan across the organization.

Here are the main reasons you must have a strong incident response plan in place:

Prepares you for emergency—security incidents happen without warning, so it's essential to prepare a process ahead of time.

Repeatable process—without an incident response plan, teams cannot respond in a repeatable manner or prioritize their time.

Coordination—in large organizations, it can be hard to keep everyone in the loop during a crisis. An incident response process can help achieve this.

Exposes gaps—in mid-sized organizations with limited staff or limited technical maturity, an incident response plan exposes obvious gaps in the security process or tooling which can be addressed before a crisis occurs.

Preserves critical knowledge—an incident response plan ensures critical knowledge and best practices for dealing with a crisis are not forgotten over time and lessons learned are incrementally added.

Practice makes perfect—an incident response plan creates a clear, repeatable process that is followed in every incident, improving coordination and effectiveness of response over time.

Documentation and accountability—an incident response plan with clear documentation reduces an organization's liability—it allows you to demonstrate to compliance auditors or authorities what was done to prevent the breach.

Source: https://www.cynet.com/

Why Multi-Factor Authentication (MFA) Is Important

Multi-factor authentication (MFA) is an IT authentication technique that requires a user to present at least two factors that prove their identity.

Why Use MFA?
Cybercriminals have more than 15 billion stolen credentials to choose from. If they choose yours, they could take over your bank accounts, health care records, company secrets, and more. Multi-factor authentication is important, as it makes stealing your information harder for the average criminal. The less enticing your data, the more likely that thieves will choose someone else to target. As the name implies, MFA blends at least two separate factors. One is typically your username and password, which is something you know. The other could be something you have. A
cellphone, keycard, or USB could all verify your identity. Something you are. Fingerprints, iris scans, or some other biometric data prove that you are who you say you are. Adding this secondary factor to your username/password protects your privacy. And it's remarkably easy for most people to set up.

Do Passwords Offer Enough Security?
We all use passwords to gain entry into our email systems, work databases, and bank accounts. We are usually forced to change our combinations periodically in the hopes that we'll stay just a bit safer. But the truth is that, on their own, passwords no longer provide an appropriate level of security. Consider Google. One password gives access to:

Email. The messages you've sent, those you've received, and the accounts you talk to are all stored in the system and protected with only a password.

Calendars. Information about who you've met, where you were, and what you did are all linked to a password.

YouTube. Your password unlocks your viewing history, your uploads, and records about videos you enjoyed.

Other web apps. Use your Google account to connect to other online resources, such as Hootsuite or Salesforce, and your password could reveal a great deal of data.

In 2017, Google admitted that hackers steal almost 250,000 web logins each week. That number could be even higher now. And each incident can be incredibly dangerous. When we think about data breaches, we often think about bank accounts and lost money. But the health care sector is also a common target for hackers. Once inside, people can change your medical records to bill fraudulent companies and make money. An altered record is incredibly difficult to change, and it could impact your health care and credit going forward.

Companies are recognizing these risks and acting accordingly. More than 55 percent of enterprises use MFA to protect security, and that number rises each year. If you haven't considered this technique, it's time to start.

Benefits of Multi-Factor Authentication
Countless organizations have adopted MFA, given the realities of today's security landscape and regulations. With compliance standards like GDPR and NIST requiring sophisticated security policies, MFA's presence will only continue to become more widespread. But given its ease of use and the protection it provides, this only stands to benefit employees and IT teams alike. What's behind the pervasiveness of MFA? There are several reasons for MFA's ubiquity in today's corporate world.

MFA Enables Stronger Authentication
Risk reduction is critical for organizations, which is why multi-factor authentication is growing exponentially. In a world where credential harvesting is a constant threat and over 80 percent of hacking-related breaches are caused by stolen or weak passwords, this kind of bulletproof authentication solution is essential.

With MFA, it's about granting access based on multiple weighted factors, thereby reducing the risks of compromised passwords. It adds another layer of protection from the kinds of damaging attacks that cost organizations millions. A security breach caused by a weak user password would understandably have huge consequences for both the company and the customers who trust it.

Passwords are a headache to remember — the more users need to remember, the lazier their password habits become. MFA secures the environment, the people in it, and the devices they're using.

Source: https://www.okta.com/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Employee Spotlight: Sully Horne

Sullivan (Sully) Horne has been our office puppy for 5 years now.

His skills include managing our deliveries to the office, supervising work in our bench room, offering cuddles and play breaks to the staff, and playing a key role in our company social media.

We're so glad to have him on our team!

Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."

FUN FACT!

preferred group IT

CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.