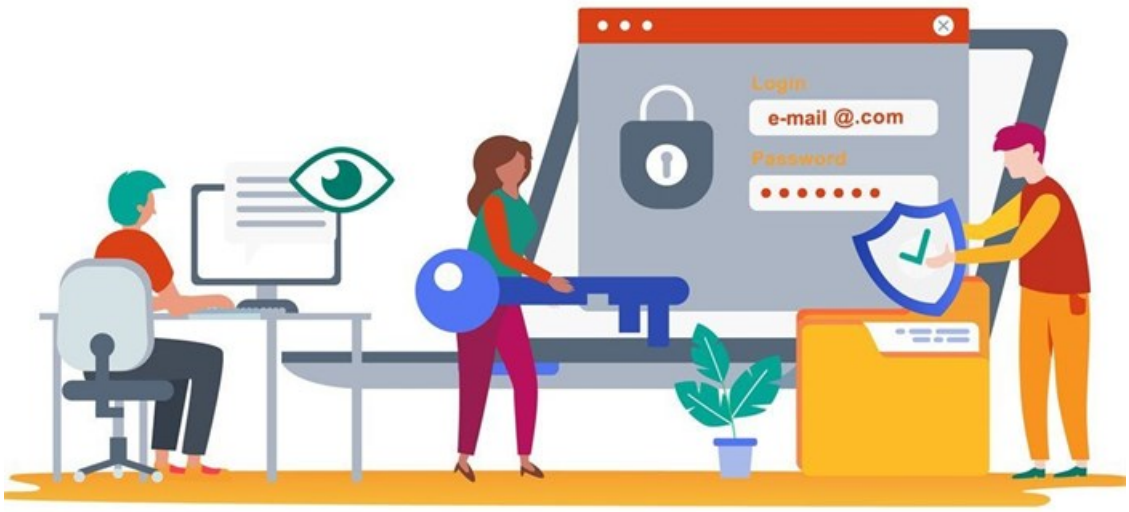
BIZCOMMUNITY

Do you have a cyber incident response plan?

This time of the year is a boom time for cybercriminals. Consumers are shopping and transacting more. Shopping websites experience higher traffic volumes and process more payments than usual. Companies security teams can often be understaffed or unprepared for the influx of spam and malware doing the rounds.



Employees are also more likely to work remotely, which often include using unsafe connections to access company networks, like mobile hotspots or public WiFi. These factors make it a great time for perpetrating cybercrime.

“Cybercrime and fraud usually spike this time of the year, running into the January lull and companies should not drop their guard with regard to security. Consumers and companies must be more vigilant over this period. Cybercriminals can target customers to steal sensitive information. For companies, the efficiency and swiftness in responding to breaches over the festive season are important for business continuity as they enter into the new year,” urges Charl Ueckermann, CEO at AVeS Cyber Security.

He says that as the cyberattacks increase in scale and frequency over public holidays and the festive season when most business-to-business organisations are not operating, as usual, cyber incident response plans become more critical to a company’s cyber defences. Poor cyber incident response not only impacts a business's continuity, but it can also alienate their customers.

“Effective cyber incident response planning will place your business in better stead for handling and recovering from cyber incidents, and minimising their impact if they do happen.”

Have policies and procedure in place

Every company with an online presence, technology systems, or email should have well-defined and communicated policies and procedures to follow in the event of a cybersecurity breach. This aids preparedness. Companies should also have firewalls, anti-malware tools, and intrusion detection in place to identify breaches and enable quick, focused responses.

“Containing the breach to prevent further infiltration is crucial following a breach. Procedures for this should be part of the cyber incident response plan. IT security teams could, for instance, take specific sub-networks offline and rely on system backups to maintain operations. During high-frequency times, like the holiday period, containment is especially important. Once contained, threats can be neutralised and systems restored to as close to their previous state as possible,” says Ueckermann.

As part of the recovery phase, the security team will need to validate that the affected systems are no longer compromised and can be restored to working condition. Timelines should be set to fully restore operations and continued monitoring should be implemented to check for any abnormal activity.

“Without an effective cyber incident response plan, that includes specific procedures to follow, it is easy to drop the ball, leading to more damage. Identifying, containing and eradicating threats as soon as possible will help to limit the impact on businesses in a time when no company can afford to have a meltdown.”

Organisations usually move into an “IT Freeze” period this time of year to focus on processing incoming commercial transactions. This makes their networks more vulnerable to cyberattacks by not updating software or patching their operating systems in a timely manner. Hackers exploit patches within a matter of days, and a proactive approach can help organisations to make it difficult for hackers to enter systems this way. Companies can’t rely solely on antivirus software for protection against threats.

“It is especially important to have an up-to-date view of the security posture of your network, know its defence capabilities and the risks to data. A company’s security posture is directly related to the possibility of a cyber incident or breach taking place. The less protection you have in place, the greater your chance is of being hacked and the greater impact a breach will have. It thus becomes imperative to take a proactive or predictive approach and to have early warning systems in place to detect potential cyber incidents. Cyber incident response is not about preventing a breach, but rather containing them to limit the damage. An internal and external vulnerability assessment of your network would be a good idea before heading into the silly season,” advises Ueckermann.

6 Tips for mitigating threats

He concludes with six tips for mitigating threats over the holidays and beyond:

1. **Understand your risk**: conduct an internal and external vulnerability assessment to know where the security gaps are in your systems.

2. **Stay up to date**: keep hardware and software protection tools up to date.

3. **Educate your people**: make sure that your employees are aware of cybersecurity risks, know your company’s policies around security, and understand your cyber incident response processes. Employees need to know how to respond in the case of a cybersecurity breach. They should know what actions to take.

4. **Implement a cyber incident response plan**: this is key to managing and minimising the damage of a breach.

5. **Proactive Monitoring**: keep monitoring your systems to identify potential risks quickly.

6. **Learn from your mistakes**: use your incident response to improve overall security. This should form part of continuous evaluation of the security posture. Knowing where your risks lie and what the impact of the risks are, is key.