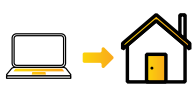
TOP 5

SECURITY RISKS FACING BUSINESSES IN THE COVID ERA

and the steps you should be taking to mitigate them.

1 INSIDER THREATS



Careless, negligent, or malicious staff represent a rapidly growing risk to all businesses. According to the Ponemon Institute, 60% of sampled organizations suffered more than 30 such incidents a year. Incidents like forgetting a company-connected iPhone in the back of an Uber, or a recently furloughed employee sabotaging a database with his still-active credentials. These incidents are not just common, but very expensive ($11.45M average cost per incident) and time-consuming (77 days on average) to contain.

WHAT TO DO

Fighting back demands investment, training, and constant vigilance. Train your staff on IT policies and procedures but also ensure accountability and enforcement. Detailed and swift employee termination procedures are critical. Leverage techniques like network segmentation, named-user accounts, zero-trust, and the principle of least privilege to limit the damage an insider can cause. Invest in monitoring tools to catch incidents before they wreak havoc, while also ensuring you have the knowledge and capacity to react to incidents quickly and efficiently.

2 RANSOM & MALWARE

Groups behind these financially-motivated attacks show little regard for the systems they disrupt and lives they impact. Look no further than the death of a German hospital patient due to a crippling ransomware attack. Municipalities, insurers, banks and countless small-medium businesses are prime targets, and with many victims opting to pay the ransom, hackers are emboldened to spread their reach and increase their demands.

WHAT TO DO

Fundamentals like anti-virus, security awareness training, spam filtering, group-policy enforcement, port security, monitoring, and automated patch management help prevent and contain potential infection. If and when an infection happens, a robust, consistently tested backup, disaster recovery, and business continuity plan with off-site replication, tabletop exercises, and network segmentation will ensure you can recover your data at the right recovery point and time without paying the ransom. Additionally, obtain cyber security insurance coverage and pay close attention to coverage stipulations.

3 SOCIAL ENGINEERING

A 600% increase in phishing campaigns since the beginning of the pandemic is no coincidence. Whether it's a Deceptive Phishing campaign masquerading as contact tracing, a Spear Phishing campaign originating from a seemingly trusted source, or CEO Fraud aiming to transfer funds in a hurry, all of these methods represent significant, proven risks to your company. As long as the human element remains the weak link in the security chain, bad actors will continue to target your staff with social engineering attacks.

WHAT TO DO

The key here is employee awareness. Mandate and test on security awareness training, utilize phishing simulations to improve detection and reporting skills, and put in place policies and procedures that clearly outline, for example, what validation steps are required when the CEO requests a bank transfer. Plus, always think before you click!

4 COMPROMISED CREDENTIALS

A quick visit to haveibeenpwned.com will probably show you that your email address is one of the 10+ billion accounts that have been compromised in thousands of past data breaches. Entire darkweb marketplaces exist to trade in these compromised credentials. Plus, thanks to poor password practices, these credentials often give attackers access to a whole host of additional accounts, both personal and corporate. Combine this darkweb free-for-all with brute force tactics like dictionary attacks and password extracting phishing campaigns, and businesses are faced with a serious threat to otherwise secure systems.

WHAT TO DO

Raise employee awareness about password best-practices, implement a privately hosted multi-factor authentication solution, enforce password expiration and complexity requirements through your directory services (Active Directory, etc), keep those same directories consistently managed, and utilize a SOC with dark web monitoring to catch new breaches and notify when credentials have been compromised.

5 SKILLS SHORTAGE

The good guys and girls are greatly outnumbered by the bad ones. With the seismic shift to remote work and the demand to secure this new cloud-delivered, laptop-based reality, the shortage was only exacerbated. Four million cybersecurity jobs need filling and there's no sign of slowing demand. Given the tight market, small and medium businesses are struggling to hire the security staff they need and when they do, they're too busy putting out fires to properly strategize a forward thinking security strategy.

WHAT TO DO

Consider outsourced services like Security Operations Center as a Service and IT Security as a Service. Instead of trying to hire full-time security staff and keep them happy, trained, and always on-call, use these services to supplement your in-house expertise at a much lower recurring and up-front cost. Plus 24x7 operation ensures that your entire IT stack is being monitored at all times for security incidents, reducing time required for threat detection, mitigation, and remediation.