IRON MOUNTAIN®

THE CURRENT STATE OF CYBERSECURITY FOR SMALL BUSINESSES

"CYBERCRIME IS THE GREATEST THREAT TO EVERY COMPANY IN THE WORLD."

Since former IBM Chairman, President and CEO Ginny Rometty said this in 2015, global cybercrime costs that were once $3 trillion per year are expected to reach $10.4T annually by 2025 – a 15% growth rate every year.

Whether it's malware, phishing, ransomware or stolen hardware, cyberattacks happen and unfortunately are something all businesses must be prepared to defend against, especially small businesses.

In a recent study, Iron Mountain found that more than 90% of business owners have someone responsible for their cybersecurity. This included 32% managing it themselves, 21% having a dedicated cybersecurity employee and 25% relying on an external IT company.

Additionally, 91% of respondents are confident in these current processes. However, 25% of the respondents still underwent a cyberattack.

Through our survey findings, we were able to identify two ways businesses can improve their cybersecurity processes and help to lower their chances of facing a cyberattack.

LOOK OUT FOR YOUR EMPLOYEE, TAX AND CUSTOMER INFORMATION

Of the businesses that faced an attack, our survey found 40% were targeted for employee records, 35% for tax records, 30% for customer records and 2 8% for personal identifiable information (PII).

To better protect this commonly targeted information, conduct a data audit to determine what information you have, pinpoint the most valuable assets and know where these records live.

Specifically, once you know where the records live, find out if they are located in a secure service, cloud storage area or saved on your computer's hard drive. If saved locally, consider transferring them to a cloud service, as most have security protocols already set in place.

The next step is to ensure your key data, based on where it lives, is updated with the latest and proper security measures. For example, ensure you have a secure firewall in place to monitor unauthorised network traffic as well as updated anti-virus software to protect from malware.

Another important element in a data audit is to determine who has access to your records and implement a dual authentication system. This provides an added level of secure access beyond passwords, allowing only those with approved authority to view sensitive information.

All these elements will allow you to have a more protected system to regularly monitor your data and be better equipped to spot threats and quickly defend against attacks.

IMPLEMENT SECURITY PROTOCOLS AND EDUCATE YOUR EMPLOYEES

When cyberattacks happen, it's easy to look to external threats, but Cybersecurity Insider found that nearly 70% of organisations say insider attacks are becoming more frequent. And when employees leave a job, nearly one-third of them take data with them.

Our survey revealed similar findings. More than 50% of business owners agree that their employees are just as much of an information security threat as external cyber threats. In fact, 60% of our survey respondents have a system to onboard and offboard employees – to respectively give and take away security access.

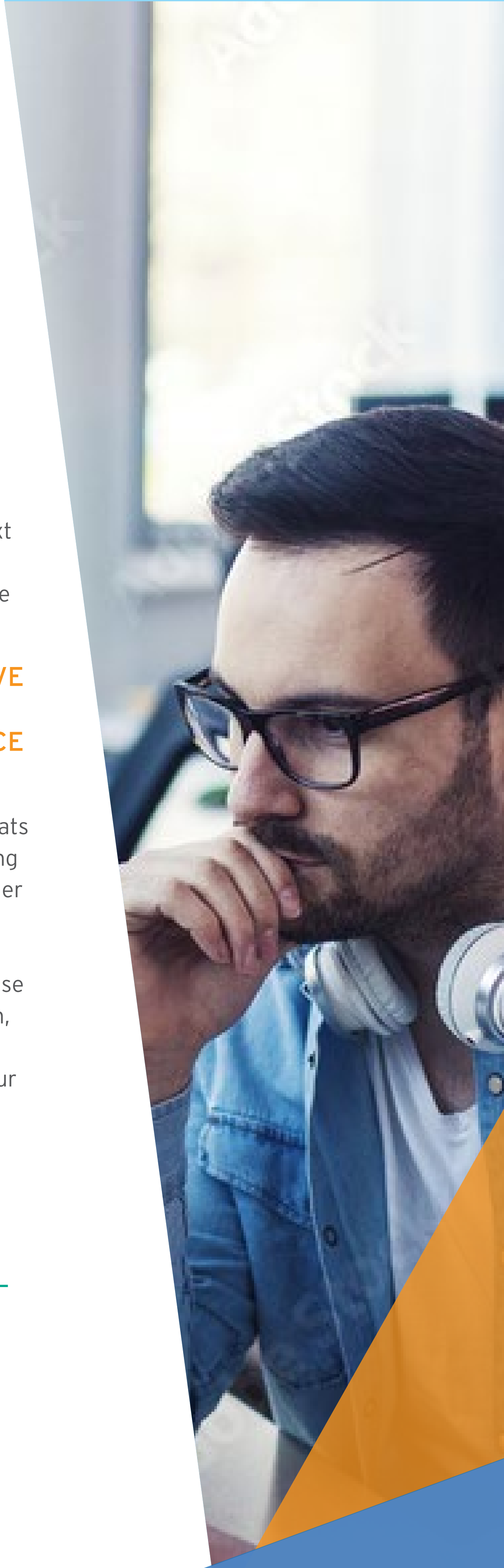
However, employees can also be your greatest asset to spot and protect against cyber threats. It's important to educate them on common cyberattack tactics to look out for. Some of the most common attacks include phishing, which accounts for around 90% of data breaches, as well as malware and ransomware attacks.

In addition, it is essential to train employees on your business's information security processes and general cybersecurity measures. For example, be transparent on the importance of your cybersecurity measures such as saving data on a secured network, and promote cybersecurity awareness courses, which can be assessed for free or at a low cost.

If a threat is identified, also confirm your employees know the proper next steps. Having a concrete emergency response plan is essential to minimise and manage your business's risk.

IT'S TIME TO TAKE PROACTIVE STEPS TO BUILD YOUR CYBERSECURITY CONFIDENCE

Many of today's business owners are not only aware of cybersecurity threats but are taking action to prevent falling prey to breaches and attacks. Consider looking to increase protection over commonly targeted records and educate your employees on a response plan if an attack does occur. In return, you'll feel prepared and confident to face any cyber threats that come your way.



+358 9 8256 020 | IRONMOUNTAIN.COM/FI
800 40 980 | IRONMOUNTAIN.COM/NO
+46 8 55 10 2030 | IRONMOUNTAIN.COM/SE
+ 45 70 21 77 00 | IRONMOUNTAIN.COM/DK

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.