IRON MOUNTAIN®

IS YOUR CYBERSECURITY STRATEGY IN GOOD SHAPE?

WHERE CAN WE FIND TODAY'S CYBERTHREATS? WHAT ABOUT TOMORROW'S? HOW CAN WE PROTECT OUR DATA FROM BOTH HUMAN ERROR AND TECHNICAL THREATS?

THE WHO, WHAT, WHY, AND HOW OF CYBERTHREATS

Tracking and predicting the nature of an attack is a massive challenge in itself. We know that threats can be malicious or simply borne of ignorance or unpreparedness. They can come from anywhere – criminals, nation states, competitors, internal human error, or even disgruntled current or former employees.

According to the 2020 Year End Report by Risk Based Security, 77% of data breaches came from outside the organisations targeted, while just over 16% came from within. The rest have yet to be determined. However, regardless of the attack vector, the end goal is usually the same – to steal intellectual property or other sensitive data for financial gain.

The one constant in this landscape is change, says John Woolley, Director of GDS Professional Services at Iron Mountain.

"A few years ago, ransomware was on the rise," he explains. "Today, many of the ransomware operations have been retired, because there simply isn't enough money in it anymore. In its place is the growth of illegal cryptomining operations." This relatively new threat involves using cryptojacking malware to leech compute power from victims to illegally mine cryptocurrency, thus severely affecting the performance and availability of victims' computing resources. "An even more serious threat is the rise of double-extortion tactics, which brings data exfiltration into the original ransomware model. Rather than just encrypting data, attackers are stealing it first and threatening to release it onto the dark web unless the victim pays a ransom," warns John.

And these are just the latest trends. Verizon's summary of reported incidents and breaches in 2021 also cites social engineering, denial of service, web application attacks, and system intrusions as other common attack vectors. In Germany, for example, the recorded number of cybercrime cases increased by 8% in 2020, while the number of resolved cases fell by 7.4%. Moreover, the pandemic stretched resources and led to competing priorities in IT and security teams as organisations very suddenly were forced to adopt remote work.

THREATS ARE EVERYBODY'S BUSINESS

Watching for these old and new threats, and challenging them, regularly falls on the shoulders of the IT team. Yet the disastrous potential effects of a cyberattack make it something that everyone in the organisation should be worrying about.

"Look at the brand damage where customer trust has been lost because personal data has been compromised," says John. "Share prices can be drastically affected, threats of prosecution from the ICO have closed companies, and fines under the Data Protection Act or GDPR can quickly finish a company."

The lesson is clear. "Businesses cannot ignore the threat," says John. "It is not a matter of if, but when."

Data protection should, he argues, be a four-stage process:

1. **Educate users** to be aware of what is happening around them, and keep educating them, because people and threats change all the time.
2. **Use technology**, such as encryption, multifactor authentication (MFA), and intrusion detection and prevention, to protect and defend against attacks.
3. **Have a disaster recovery plan** that is regularly tested and updated and ready to go if the worst happens.
4. **Dispose of IT assets properly** to ensure that data previously stored on retired data-bearing devices can never be recovered.

TRUST NO ONE

"The weakest link is human behaviour," says John. Phishing and its evolving variants, for example, successfully exploit human vulnerabilities though mass and targeted attacks.

"Social engineering as a form of attack is huge," says John. Fooling people into clicking on a malicious link, for example, has moved from the now well-known executable files to techniques like embedding links in spreadsheet macros or spoofing legitimate links.

There is only one answer. "To combat this," says John, "everyone should be working on a zero-trust basis. If something happens out of context, question it. Never trust, always verify."

HOW MUCH DATA DO WE REALLY NEED TO KEEP ONLINE?

As IT professionals, we already know much about the technology solutions needed to protect our data, not least of which is enterprise-grade security software and its associated high cost.

But what about the data itself? We know we now have the means to keep vast quantities of data readily accessible, but should we?

"The more data that's held online, the more there is to steal," John argues. "It's like displaying all your valuables in the window. The glass might be double-glazed, and there's a guard dog, but it's still right there on view."

Instead, we could adapt tried and tested strategies to protect more of our data by taking it offline. Making regular copies of data to store offline and off-site is a valuable tool in the disaster-recovery armoury. Even greater data security can be achieved by using an airgap to store data in total isolation, away from vulnerable data and impervious to attack. That way, the business can be confident that, as it gets up and running again, it's doing so with unaffected data.

Taking more data offline means businesses need to look at the data they hold and determine just how accessible it needs to be. Are real-time analytics using old data actually contributing to the business? Does HR really need instant access to data on former employees? Does great customer service really require every byte of customer data to be right there at an agent's fingertips? Do remote workers really need access to every single app and database? During the pandemic, many remote workers have been granted access to apps and data they do not actually need to perform their roles.

For data that must be kept online and available, applying encryption is essential for protecting it from theft. This is especially important when double-extortion tactics, in which sensitive data is also exfiltrated and its owners held to ransom, is on the rise. Moreover, organisations should apply digital rights management to unstructured content. Finally, if the data is not needed but could potentially have value later on, then it should be taken offline and archived.

There's a financial argument here too. John explains "We know that software and data storage account of some of the greatest expenditure in IT. If we can tackle the cost of data storage, then that budget comes back to use elsewhere."

CHANGING MINDS AND STRATEGIES

As John points out, "The six most expensive words in IT are said to be 'We've always done it this way'."

With threats constantly evolving, that means taking cyberthreats seriously, reassessing how users and technology handle data, and changing our ways.

References
"2020 Year End Report Data Breach QuickView," Risk Based Security
"2021 Data Breach Investigations Report," Verizon
"Cyber Security Breaches Survey 2021," UK Government

08445 60 70 80 | IRONMOUNTAIN.CO.UK
R.O.I. 1800 732 673 | N.I. 08445 60 70 80 | IRONMOUNTAIN.IE

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 organizations 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 centers, art storage and logistics, and cloud services, Iron Mountain helps organizations 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.

© 2022 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.