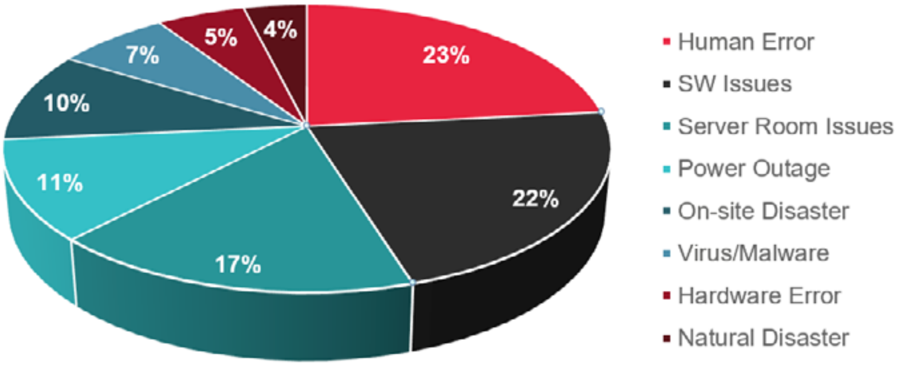
UNITRENDS

DISASTER RECOVERY TECHNIQUES THAT STOP THE ENEMY WITHIN

FIVE EMPLOYEE HABITS THAT THREATEN YOUR BUSINESS

INTRODUCTION

Most reports on data protection and business continuity highlight the need for vigilance against external threats. You read a lot about the negative business impacts of hurricanes, tornadoes, earthquakes, fires and malware, but a different class of threats are far more prevalent – those created by your own employees.

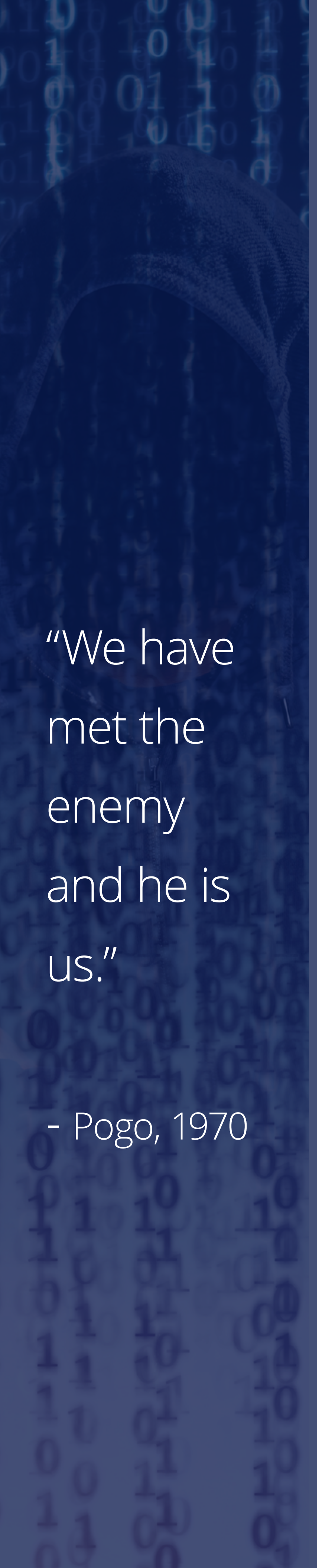


*Source: CRN Magazine

As seen in the CRN study above, employee error ranks as the number one cause of business interruptions. There is also a large human factor in most other IT downtime incidents; for example it takes just one employee clicking on a shady link to initiate a ransomware attack.

Your data protection and business continuity strategy must be able to handle both external and internal threats. Here are five examples of employee data protection challenges and guidance on how your business continuity solution should handle them.

EMPLOYEE THREATS



"We have met the enemy and he is us."

- Pogo, 1970

#1 – Premature Code Launchers

According to the CRN report, the number two cause of business interruptions is software errors. These includes software patches that introduce more issues then they fix, upgrades that break links to integrated systems, systems that hang, and uncontrolled restarts. While software vendor releases are marketed as being production ready, you never really know how they will perform until they are installed in your unique production environment.

The most prudent approach to keeping software issues from causing business interruptions is to test all changes prior to being released onto production systems. Companies should utilize data protection appliances that offer copy data management (CDM). CDM allows administrators to instantly create isolated, fully featured test and development environments from backups. These test/dev environments can then be made available over the network for software version testing, analytics, patch tests, or what/if analysis without risking production environments. By using a CDM approach to testing, any issues with software patches will be discovered during testing and ensure the corrected version will run as planned in production. Using CDM for testing may reduce the need for additional storage and dedicated infrastructure to spin up test labs.

Systems with advanced CDM have the ability to do security scans on backups before bringing up a test / dev environments. You should always follow your security best-practices, but you may find that certain machines are too impacted to scan for viruses in production. CDM with integrated security capabilities allows you to perform this function before building a test environment. This additional layer of security will minimize malware and virus infections and make no demands on your production environment.

Being realistic, some bad code will still slip through so organizations still need the ability to quickly and easily roll back software to the last functioning version. However, preventing bad software from being deployed in the first place will reduce negative impacts on business processes and employee productivity.

#2 – Malicious Employees

The frequency of malicious employees purposefully harming a company are difficult to measure as organizations are reluctant to disclose these events. It is an embarrassment to admit bad hiring practices or that relations with an individual have been allowed to degrade to the point of them wanting to harm their company. A recent analyst report indicated that a major triggering event for employees to maliciously delete Office 365 data is a company merger or acquisition. Today, with fully automated business processes employees with overly broad security privileges are in a position to do great harm by deleting large volumes of data or purposefully introducing corrupting software. The most dangerous aspect of insider threats is the fact that the access and activities are coming from trusted individuals, and thus will fly below the radar of many detection technologies.

One important tool to limiting the potential negative impact of an employee is to limit their access to only the data they need to do their job. Data protection tools with Distributed Enterprise Management (DEM) allow backup administrators to grant role-based management rights to limited content in the enterprise's collection of backups. DEM enables managed self-service, freeing IT from that work, and limits visibility to data from other parts of the organization.

The most common employee attack is to intentionally delete software, files, emails and SharePoint folders prior to their termination. Organizations can protect themselves from this form of attack by using data protection systems that backup the entire software stack, (server

settings, data bases on remote servers, and operating systems) as well as have infinite and remote data retention. Recovery can then be just a few clicks away.

#3 – Ransomware Clickers

On the list of leading causes of lost business productivity is virus / malware attacks. All employees are potential ransomware clickbait. Corporations should conduct employee training to educate their workforce on how to identify and avoid potential infections, however it only takes one bad click to launch an attack.

An additional problem is that new ransomware variants are emerging every day. Your ransomware protection needs to continue to evolve to keep up. Enterprise data protection appliances should have the ability to quickly and accurately identify ransomware activity as part of every backup. New ransomware variants operate in stealth mode, seeking critical files, and encrypting at a slower rate to stay under the detection radar and increase the odds that a ransom will be paid. Newly developed artificial intelligence (AI) runs during every backup, analyzes the randomness of file changes (not just change rates) and identifies backups infected by ransomware. Upon detection, email and dashboard alerts should be sent immediately to administrators, and all suspected backups flagged with icons to prevent attempted recoveries using infected files.

#4 – Data Hoarders

Dealing with data growth is difficult. The storage capacity of servers needs to support highly virtualized environments, with potentially dozens of applications running at the same time. Purchasing SANs or NAS devices is expensive, especially for small and mid-sized organizations. Industry and government compliance requirements say that some data types need to be preserved and for 7-10 years or even forever. On average organizations can expect data volumes to grow 10% per year, compounding into TB-sized data sets over time.

There is a set of employees that literally save every shred of data, email, file, doc or PPT they come across in the belief that there is a slight chance they may need it again in the future. Keeping all this data on spinning disks is expensive. Long term data storage in the cloud is particularly effective in preserving data files against local failures and inadvertent deletion. The cloud can store data at a lower cost per GB than on-premises solutions. Organizations of all sizes need their backup appliances to have seamless integration with the cloud so archiving and data compliance can be programmed and continue with no human interaction.

Organizations must also ensure that their data protection appliances are scalable to handle larger storage volumes as the business grows. When considering a new data protection appliance be sure and forecast the data volumes you will need to protect over the life of the product.

#5 – Sloppy Employees

This last category of challenging employees is just about all of us. There are few of us that haven't inadvertently, or in a fit of organizing frenzy, lost or intentionally deleted important files. Almost every IT professional can tell you about calls they receive declaring that "An important file is missing and have no idea of where it went or who could have lost it!" Lost file recovery is one of the most common tasks and can chew up many hours of IT time.

Organizations need to ensure their data protection appliances support easy file recovery; it should take less than five minutes to recover a lost file, from login to full restoration. The UI should be easy and intuitive enough that any member of IT can recover a lost file without having to consult a manual or receive special training. Quickly addressing these interruptions will enable IT to focus on more pressing organizational projects.

New ransomware variants operate in stealth mode, seeking critical files, and encrypting at a slower rate to stay under the detection radar and increase the odds that a ransom will be paid.

CONCLUSION

Now that you have heard about threats to your business posed by your employees, is it time ensure that you can deal with them as part of your data protection and business continuity strategy? You may be interested in seeing how Unitrends is deploying these capabilities for Simpler, Smarter IT.

Other Items that May Interest You:

5 Minute Disaster Recovery Checkup

Get a personalized disaster recovery report for your environment.

Read More

INTRODUCTION

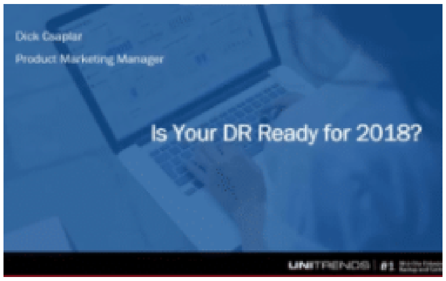
IT Administrators are responsible for the technology that keeps the world's businesses running. Every day they are faced with circumstances threatening to bring down your applications, servers, and even communication. IT is forced to recover from catastrophic weather events, hardware failures, advanced ransomware infiltrations, and hundreds of other potential disasters. Even a minor event in just one of the millions of components in a modern datacenter can ripple out of control and cause enterprise-wide problems.

The cost of failure is high. Failing to recover or deflect the attacks results in application downtime. While the cost downtime on your business varies dramatically across industries, an average for all organizations is about $9,000 per minute. While 99.9% uptime is great, shortening that to 99.99% saves the average organization about $350,000 per month. This level of uptime is only possible if data protection and business continuity

Thriving in Threatening Times with IT Resilience

The next stage of the business continuity evolution is called IT Resilience (ITR). ITR includes building smart, self-directing capabilities into applications as well as the IT infrastructure. Here are 5 steps you can take today to achieve IT Resilience.

Read More



Dick Csaplar
Product Marketing Manager

Is Your DR Ready for 2018?

Get Your DR Plan in Shape for 2018

Five Questions, Four Calculators, and One Test to prepare you for the new year.

Read More

TEST YOUR THREAT IQ

Unitrends increases uptime and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a "one throat to choke" set of offerings that allow customers to focus on their business rather than backup. Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

*CRN http://www.crn.com/slide-shows/storage/240006796/8-surprising-disaster-recovery-stats.htm/pgno/0/7

unitrends.com
PART# WP-2071-ENG-A-the-Enemy-Within

UNITRENDS