OUT IN FRONT PLAYBOOK

FEBRUARY 2022

EMBER™

EMBERIT.COM

THE FOLLOWING CONTENT MAY BE CONCERNING

THAT'S WHY WE'RE HERE

In recent years, as companies embrace both expansion and a new world of remote work, cloud computing has become ever more present in our professional lives.

The good news: employees are connected by virtual meetings, remote access, and shared spaces. The bad news: all of that can seem like easy access points to bad actors. The threat that comes along with cloud computing grows and for many, it's enough to make you want to put your head down and ignore the risk to your business.

The first step towards protection is awareness and acknowledgement and we're here to help on both fronts. We're also in the business of keeping our heads up and facing threats to help both our company and our clients stay out in front of an ever-changing landscape. We know it's not easy to stay on top of cybersecurity but we believe that together, we can do it.

Read on for key ways to improve your cloud security and to help address burnout on your team - and give us a shout when you're ready to get your business out in front of cybersecurity threats.

Chris DiFonzo

Chris DiFonzo
Chief Executive Officer
cdifonzo@emberit.com

THREAT SPOTLIGHT

THE FALSE SENSE OF CLOUD SECURITY

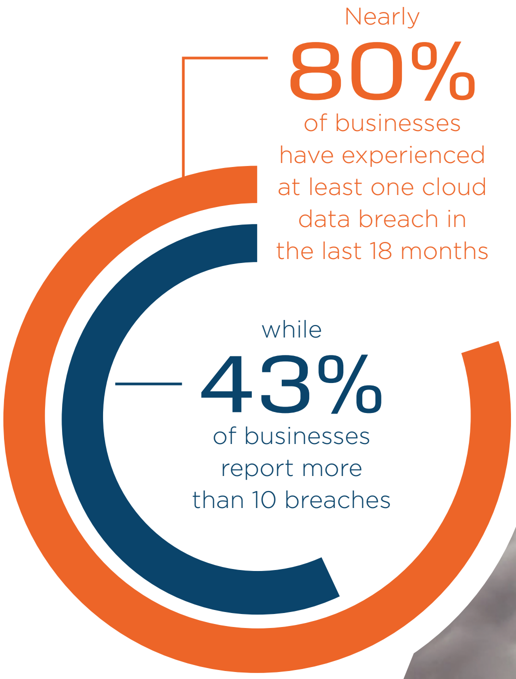
In a world where most people are looking for easy solutions and companies are looking to innovate, the idea of "the cloud" is often touted as a collaborative solution for growing organizations, distributed workforces, and blended teams. While on-demand access to resources, documents, and information can have a positive impact for many teams, it is by no means a comprehensive or always secure solution. **Cloud computing** brings with it a set of unique challenges that must be weighed against the overall benefits it adds for your organization.

n. The on-demand availability of computer system resources, especially data storage and computing power, and materials without direct active management by the user.

As with any repository, who can access your materials and when are key components of managing security. When it comes to the cloud, ease of access for your employees also means easier access for bad actors. Access on a closed network, while less convenient, allows you control of the wifi used to access the data. The "access from anywhere" benefit of the cloud offers no such control and as we all know, simply connecting to an unsecured wifi network is a wide open door to bad actors.

Beyond the access issue, cloud solutions also bring any security risk that comes with the cloud provider. Most cloud services are run by third parties, so your data and information inherently becomes subject to risks that come along with that provider. When moving to cloud storage, it's imperative to understand how your provider manages data security, what they do in case of a breach, and how they view security ownership. Many third party providers see security as a shared responsibility and only take partial credit for maintaining that security. Third party providers may also become their own risk center as they grow and gain prominence. By partnering with a cloud provider, your organization is taking on additional risk. It is every organization's responsibility to understand what data they are housing in the cloud, who can access that data, and how it is protected.

Though some solutions offer effective security measures like multi-factor authentication and limited access settings, these are often circumvented in the name of convenience. If you've decided to use a cloud solution, make sure to incorporate additional security constraints and provide access protocols for your staff. Educating and informing your employees can go a long way in preventing data breaches on your cloud solution.



Nearly **80%** of businesses have experienced at least one cloud data breach in the last 18 months

while **43%** of businesses report more than 10 breaches

Source: Ermetic

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

The Mascot Minders are a small distributed team of pet trainers that work exclusively with the animal mascots of major league sports teams. Because their work requires them to travel frequently, they've incorporated a cloud-based storage system for their entire business - everything from invoicing and payments up to pet training protocols. They use a popular cloud storage provider and do their best to manage access from both employees and clients.

Upon signing a popular East Coast hockey team, the Minders follow their standard protocol of sharing onboarding information and invoicing with their new client contact. Things were going well until their tech-unsavvy client had trouble accessing the needed information. Not wanting to slow things down, the Minders made a one time exception and sent an open access link to the client. Unfortunately, they failed to close the loop and tighten the access back up after the download.

Six months later, Mascot Minders suffered a significant breach with bad actors downloading payment and contact information for major league sports teams across the country. Many of their clients chose to terminate their contracts due to the fallout and Mascot Minders was forced to lay off a number of their staff.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

Top 5 Security Risks Of Cloud Computing And Strategies To Mitigate Them
simplilearn.com // 12.08.21

Cloud Security Threats: Definition and Explanation
vectra.ai

Top Cloud Computing Security Challenges
cybersecurity-automation.com

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THREAT SPOTLIGHT: CLOUD COMPUTING

PLAYBOOK

5 TIPS TO KEEP YOU OUT IN FRONT

EDUCATE YOUR EMPLOYEES

Your team is one of the biggest risk factors when it comes to cloud computing. Include the whole team in security training, create a protocol that is regularly updated, and consider periodic tests to ensure things are running as smoothly as possible.

SECURE YOUR DATA

Cloud storage offers anytime and anywhere access but data or document loss is a real concern. Integrate regular backups into your process to ensure you don't lose your most important assets.

MANAGE ACCESS

Not every employee needs access to every document. Outline a protocol for granting access to documents and folders and maintain access points diligently.

UTILIZE ENCRYPTION STRATEGICALLY

Just because it's on the cloud doesn't mean it has to be available to anyone. Incorporate additional password protection and data encryption on your most sensitive information.

INCORPORATE MULTI-FACTOR AUTHENTICATION & PASSWORD PROTECTION

Just like any storage resource, many cloud providers will allow you to set requirements for passwords and MFA. Use them!

FEATURED PARTNER SOLUTION

Installing "state of the art" security technology gives us a sense of … well … security, but the scary truth is that attackers effortlessly bypass such efforts every day, inflicting untold damage to businesses across every size and industry.

The security teams tasked with combating these breaches are bombarded with hyped-up products and services that can easily lead to more spending that might not even offer more protection. What would be truly helpful would be an ally that businesses could count on to make what's critical, easily accessible, to provide answers along with alerts, and service informed by real-world expertise.

Red Canary is that ally.

The human-powered platform behind Red Canary delivers superior threat detection, hunting, and response capabilities across endpoints, cloud deployments, and network devices. By removing the need to build and manage a 24/7 threat detection operation, they help teams focus on running business securely and successfully.

The bottom line? Red Canary customers see 95% reduced **alert fatigue**, 10x faster response, and a 3.8x increase in confirmed detections — and all of that adds up to greater confidence in their security programs.

THE RED CANARY APPROACH

DETECT

Advanced threat detection by combining machine learning with human ingenuity and an always-on threat hunting team

INVESTIGATE

Contextualized and actionable alerts that weed out false alarms

RESPOND

Pre-planned protocols allow swift and thorough response to mitigate damage and down time

IMPROVE

Round-the-clock vigilance to detect and learn more about new threats and actors

RED CANARY

YOUR SECURITY ALLY

OUT IN FRONT OF

Information Security

WHAT RED CANARY DOES

Red Canary enables your team to focus on the highest priority security issues impacting your business. By removing your need to build and manage a threat detection operation, we help you focus on running your business securely and successfully.

INDUSTRIES SERVED

▣ Financial
▣ Food & Beverage
▣ Health
▣ Manufacturing
▣ Legal
▣ Technology

BEST FOR

COMPANIES OF ALL SIZES LOOKING FOR ALWAYS-ON PROTECTION, BUT ESPECIALLY LARGE AND DIVERSIFIED ENTERPRISES

n. when admins or analysts receive an overwhelming number of alerts from security tools — some of which are innocuous and irrelevant — causing them to ignore the alerts that really matter.

THE SECURITY COST OF BURNOUT

SUPPORTING YOUR TEAM THROUGH TIMES OF STRESS

We all know that humans are behind the majority of breaches - and when we're tired and overwhelmed, we're much more likely to miss obvious signs of security issues.

Burnout is an increasing factor in cybersecurity and unfortunately, burnout doesn't just disappear with a new week, new month, or new quarter.

With the rapidly changing landscape of cybersecurity and the ever-evolving nature of security threats, our field is one that is in particular danger when it comes to burnout. Executives, team members, and everyday citizens are exhausted from the hypervigilance that can be required to keep their data, organizations, and team members secure. Add on the stress of our everyday environments and the shortage when it comes to talent, and we've got a threat almost as large as actual data breaches.

One major driver of burnout within the cybersecurity industry is the belief that all risk is of critical importance. In reality, we know that not every risk is equal and that to make the biggest impact for our organization, we sometimes need to focus on the risk that can drive the biggest impact. This doesn't mean that we ignore small risks but that we decrease the hypervigilance required to address each threat with the same speed and depth.

Additionally, we see many cybersecurity leaders taking on too much responsibility alone. Cybersecurity should be a team sport, with multiple team members contributing and bearing the load. Building a cybersecurity taskforce within your organization can go a long way in preventing burnout and in fact, can strengthen your entire cybersecurity process. When all responsibility and internal knowledge is heaped onto a single set of shoulders, you effectively create another threat for your team.

Even in situations where your team is limited, building processes and adding resources can be a way to combat burnout. Tools are important to supporting your cybersecurity practice but they will be nearly useless if your team isn't well trained to use them and armed with resources that make the most of their time. Build a foundation to help your human power make the most of their time and to work efficiently.

It's important to acknowledge the impact of burnout on ourselves and our teams and build resilient habits to keep ourselves - and our security practices healthy. Encourage your team to address concerns of burnout and to discuss this issue without repercussions. As a team, we can help to expand coverage but also address burnout head-on by communicating openly and effectively.

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Kate Beckett is the Chief Security Office of Castle Healthcare, a small hospital network in New York with a collection of hospitals and clinics. Because she works in the healthcare space, Kate is vigilant about staying up to date on cybersecurity trends and the latest threats impacting her industry - so up to date that she hasn't taken a day or even an evening off in months.

While Kate has a team of security-minded professionals at her disposal as well as an organization that knows cybersecurity is important, she feels the pressure to manage and monitor every incoming threat herself before sharing it with her team. She often finds herself behind in the monitoring of threats and feels overwhelmed by the attempt to do it all.

One typical Friday night finds Kate trying to catch up on her security reports while multitasking at home. She's deep in the middle of a new report when takeout arrives. She files the report without fully reading it and continues on with her evening.

When Monday morning arrives, Kate is called into a leadership meeting where she learns that the hospital has been hit with a security attack, leaving countless healthcare professionals unable to access patient files, surgery schedules, and more. Thinking back, she realizes that the Friday report had outlined increased malicious activity within the hospital's networks and recommended action for her team to take - but she'd glossed over the recommendation in the face of so many frequent threats.

It takes Castle Healthcare days to get back online and while they're able to resolve the threat quickly, the damage has been done. Patients are less willing to trust Castle with their healthcare needs and their data, doctors and nurses are anxious about future incidents, and Castle leadership is frustrated with what they see as a gap in Kate's vigilance. Kate identifies the burnout issues inherent in the situation but is unable to make headway in creating a process for identifying burnout within the organization and soon leaves for a position at another healthcare network.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

Cybersecurity Burnout
stronger.tech // 02.20.19

Burnout in the Cybersecurity Community - Security Through Education
social-engineer.org // 12.08.21

Facing Tech Burnout? Here's How Employers Can Help
securityintelligence.com // 10.26.21

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THE HUMAN FACTOR: BURNOUT

PLAYBOOK

6 TIPS TO KEEP YOU OUT IN FRONT

DEFINE YOUR CYBERSECURITY PRIORITIES (AND ACKNOWLEDGE RISK)

As with any important business process, it's crucial to outline your cybersecurity priorities as an organization. What are you trying to accomplish in the next business period? What matters most to your team? How will you measure your results? Aligning on these priorities helps your team focus on the areas that matter most rather than spending their time chasing every minute risk that rears its head.

BUILD A ROBUST TEAM OF CYBERSECURITY LEADERS

Cybersecurity shouldn't fall to a single person on your team but rather, should be the job of all employees. By building a wide delegation of cybersecurity leaders within your organization and arming them with the tools they need, you'll effectively spread out the pressure of the work and help to avoid single employee burnout.

SUPPORT YOUR TEAM WITH RESOURCES & TOOLS

In addition to spreading the wealth when it comes to cybersecurity ownership, tools and resources can go a long way in helping to avoid burnout within your organization. Providing the right tools, training, and processes for your employees to navigate cybersecurity limits the amount of time they will be searching for guidance or answers.

FOSTER OPEN COMMUNICATION

We can do our best to mitigate the threat of burnout but it's unlikely we'll eliminate it altogether. Creating an environment where your team feels comfortable addressing burnout can help to address issues quickly and avoid the threats that come from long-standing exhaustion.

ENCOURAGE BALANCE

Similarly, encouraging your team to find balance at work (and outside of work) helps to alleviate the stress that comes with high import jobs like those in cybersecurity. Help to model best practices when it comes to balance, priorities, and hours so your team can do the same.

BUILD A PROCESS TO IDENTIFY BURNOUT

Lastly, take the time to construct an internal process for proactively identifying signs of burnout so you can address them as needed. Watch for employees who seem disengaged or those who are taking numerous sick days (physical health is also often impacted by burnout) and develop processes and resources for the employees that need them.

{ OUT IN FRONT WIN }

HOW MICROSOFT STOPPED THE BIGGEST EVER DDOS ATTACK

Cybersecurity attacks are becoming more frequent and more costly with each new year. Phishing attempts, ransomware attacks, data breaches, and distributed denial of service (or DDoS) attacks are all on the rise and can take considerable time and energy to remedy after they've hit. If there's any silver lining to increased attacks, it's that many companies are taking cybersecurity seriously for the first time and others are stepping up their protections and responses when it comes to threats.

Case in point: Microsoft's response to an unprecedented DDoS attack in November 2021. In fact, Microsoft was able to stop the largest ever DDoS attack to date - a record 3.47 terabytes per second (TBps) which exceeded the previous record of 2.4 Tbps DDoS.

DDoS attacks are especially pervasive as they harness the power of connected devices and data to take a specific target — usually a website or internet service — offline, resulting in a literal disruption of service. They're also becoming incredibly common, much like other cybersecurity threats. Microsoft's Azure team noted that in addition to November's record breaking attack, they also thwarted two different 2.5+ TBps attacks in December 2021.

The record-breaking 3.47 TBps attack was classified as a User Datgram Protocol (UDP) reflection attack where "UDP request and response packets are reflected within a local network using a source Internet Protocol (IP) address that's been spoofed by the attacker." These types of threats are perpetrated by a bad actor who abuses UDP by creating a valid UDP request with a false IP address and reroutes response packets from the target IP address to the attacker's IP address. In 2021, 55% of DDoS attacks relied on UDP spoofing.

A **reflection attack** involves an attacker spoofing a target's IP address and sending a request for information, primarily using the User Datagram Protocol (UDP).

Though these attacks are often very short in duration (10-15 seconds), they strategically target industries, processes, and workloads where a brief disruption can do a lot of damage. Common targets include online-gaming servers, streaming applications, and similar systems. The gaming industry specifically has been hit with multiple DDoS attacks and numerous games have been impacted.

Like most cybersecurity threats, DDoS attacks can be at least partially prevented by having the right processes, protocols, and protections in place. Learning from unsuccessful attacks such as this 3.47 TBps one can help us move our protections forward and help us all learn to be strategically prepared.

EMBER™

Delivering best-in-class cyber security, IT management, and consulting services to small-to-mid-sized businesses

EMBERIT.COM