CybelAngel

INDUSTRY ALERT

Reducing Data Breach Risk From Your Increasingly Remote Workforce

WWW.CYBELANGEL.COM

TABLE OF CONTENTS

Reducing Data Breach Risk From Your Remote Workforce

Introduction

The number of remote workers around the globe climbed exponentially in response to the Covid-19 pandemic. With this redistribution of workforce to home offices and kitchen tables comes a substantially increased opportunity for exploitation by threat actors. This shift to a workforce outside of the enterprise's perimeter impacts all organizations—from those with robust information technology infrastructures and protocols to those still early on in their cybersecurity journey.

These new remote workers are accustomed to conducting business inside their company's firewall and being protected by the company's cybersecurity policies and practices. Without these safeguards, remote employees are more likely to inadvertently expose sensitive data, including employee or customer credentials, intellectual property, or personally identifiable information (PII).

Many data leaks resulting from remote working will be entirely accidental, with well-meaning employees exposing documents or data during the course of performing their usual tasks from a home environment. Law firm Baker McKenzie shares that, "In such an environment, employees may make assumptions that they have wider latitude to email, copy, send, print, or download information, given the circumstances. **Compounding these insider risks are a series of unknowns,** such as whether your employees' home networks have security anywhere near on par with in-office network security that could allow outsiders to intrude or access data."[1] These risks could be exacerbated by the rapid adoption of online communication and collaboration tools, which occurred at an unprecedented pace in the first quarter of 2020, with Slack® adding 7,000 new customers between February 1 and March 18—more than they had in the entire previous quarter.[2] Microsoft® announced in early March that the number of daily users for their Teams offering grew to 44 million,[3] and the number of meetings grew over 500% since the end of January.[4]

The potential for a negligent data leak to impact an organization is significantly increased given this unprecedented shift to a primarily remote global workforce. This paper provides analysis of several risk vectors that are on the rise as a result of the shift. It also provides tips from cybersecurity experts on how risks can be minimized, leaks identified quickly, and remediation completed without undue strain on information security teams.

[1] William (Bill) F. Dugan & Christine M. Streatfeild, *Keep Trade Secret Protections Top Of Mind While You Deploy Remote Working*, Baker McKenzie (2020), https://www.bakermckenzie.com/en/insight/publications/2020/03/trade-secrets-remote-working-covid-19

[2] Alex Wilhelm & Natasha Mascarenhas, *Slack adds 7K customers in 7 weeks amid remote-work boom, besting its preceding 2 results*, TechCrunch (2020), https://techcrunch.com/2020/03/19/slack-adds-7k-customers-in-7-weeks-amid-remote-work-boom-besting-its-preceding-2-quarters-results/

[3] Taylor Soper, *Microsoft Teams hits 44M daily active users, spiking 37% in one week amid remote work surge*, GeekWire (2020), https://www.geekwire.com/2020/microsoft-teams-hits-44m-users-huge-37-growth-spike-1-week-amid-remote-work-surge/

[4] Jared Spataro, *Our commitment to customers during COVID-19*, Microsoft.com (2020), https://www.microsoft.com/en-us/microsoft-365/blog/2020/03/05/our-commitment-to-customers-during-covid-19/

Understanding the Data Breach Risk

As organizations and their employees adapt to new remote working conditions, cyber risk will increase with the expanding cyber attack surface. CybelAngel analysts have identified three risk categories to assist security teams in focusing on this increased risk, along with tips for actions to limit exposure and impact.

SHADOW IT

Shadow IT refers to employees' use of tools not explicitly authorized by the IT department of an organization. The adoption of shadow IT is commonly motivated by one of three factors:

1. Need for a tool not currently provided,
2. Desire to improve ease and efficiency of work, or
3. Perceived need to circumvent existing security protocols to complete work tasks.

Many employees in search of alternative solutions to authorized tools will opt for free subscription plans, which often do not include the same security and privacy controls as those plans designed for integration by IT teams. This situation is likely to occur with greater frequency when employees have a perceived greater autonomy when working outside of the company's firewall, and increases the probability of sensitive data leaks.

Shadow IT Example

To ease the transfer of information with multiple third-party vendors, a resourceful group of employees set up their own server using a standard NAS drive, without authorization for their IT team. The web interface these employees used was secure, but the NAS drive itself was not. This resulted in shared files being publicly accessible, jeopardizing a 5-year, nearly half-billion-dollar project that had been in development.

Pro Tip: Proactively Accommodate Your Employees

Now is a good time to remind employees about corporate cyber security policies. While every company has their unique policies, some general reminders to share might include:

- Do not permit employees to install unauthorized plugins or extensions to browsers or systems.
- If your organization has an IT helpdesk for employees to request new tools or ask about a plugin or third-party app, it might be time to re-share the contact process.
- Last, but not least, simply remind your workforce of the dangers of shadow IT.

Progressive IT organizations have also begun proactively surveying their employee base about new or additional tools and systems that might make their work product better, stronger, or faster. This strategy helps adapt approved corporate technology stacks and avoid unpleasant shadow IT surprises.

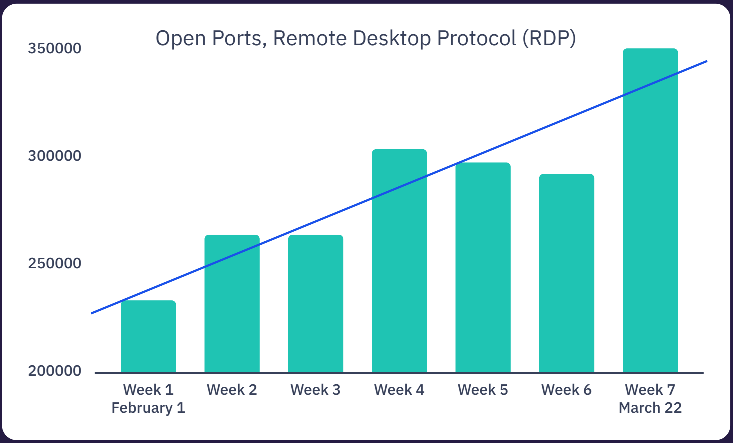
HOME NETWORK VULNERABILITIES

Many home wireless networks are fit for their usual intended purpose—allowing the household to browse the web, share photos, or tether their mobile devices. They are not, however, necessarily well suited to protecting sensitive business data and preventing data leaks. As remote working increases, employees are likely to be using their existing home wifi to access corporate networks, retrieving and perhaps locally saving sensitive information. Risk factors may include routers with outdated software, or IoT devices left on public default settings. Compounding these risks is that organizations have been rushed into remote work, without having the time to provide proper employee training regarding cybersecurity best practices.

Remote Workforce Workarounds

For companies that do not yet have a VPN in place, enabling employees to work from home can mean relying on Remote Desktop Protocols (RDP). While this tool allows for collaboration between offsite employees, it brings with it the risk of ports being left freely accessible to outsiders.

CybelAngel analysts reviewed data to determine the number of unsecured RDP ports observed from the start of February until late March 2020. Findings show that the number of open ports is on the rise, with weekly average of open ports growing by over 50% during this time period, from 233,375 for the first week of February, to 351,350 the week ending March 22, 2020.



Pro Tip: Facilitate Access While Providing Guidance

- Encourage employees to provide details on the at-home devices they are using so that compliance with your security policies can be confirmed. A quick Nmap scan may reveal open ports and allow protection to be validated.
- Educate employees on the importance of changing the default passwords on their networks and devices.
- Be sure to give the correct access to the right people. As a security administrator you may want to ease the connexions to the company's servers, but it doesn't mean you have to remove security: keep login portals, define correct rights, and double-check incoming connexions. IP whitelisting (or blacklisting, defined on countries) could be an option.

GOOD ENVIRONMENT FOR PHISHING

Attempts made to gain valuable information, such as credentials, PII, or critical business information, have increased during the transition towards remote working. Cyber threat actors are launching new and innovative threat campaigns, socially-engineered to take advantage of the rapid change in employee circumstances.

A natural reaction to receiving an odd email might be turning to an office mate to get their input, or to remind them to be on the lookout for a similar email; however, it can be difficult to maintain a culture of information-sharing about phishing attempts with employees dispersed to home offices. Employees are more likely to fall prey to phishing attacks, such as an urgent email purporting to be from senior leadership. By creating a sense of urgency, this email may not get as critical a review as it would if the employee were in the office, and an employee may accidentally jump into action and leak sensitive data. Other phishing attack techniques on the rise include threat actors impersonating your organization to gain a prospect's or client's data.

Shadow IT Example

Threat actors have employed a variety of phishing campaign forms to take advantage of newly remote employees' uncertainty and anxiety. Covid-19-related phishing campaigns have incorporated fraudulent offers of social services, impersonations of governmental agencies (including the World Health Organization)[5], and relief donation scams. What's more, the volume of these phishing campaigns has risen quickly through Q1 2020, as estimates indicate nearly a 700% increase in Covid-19-related phishing attacks from February to March.[6]

Pro Tip: Refresh Awareness and Keep an Eye on the Horizon

- Launch phishing awareness programs to help employees identify the latest attempts being made, either towards your organization or others. Making the issue top-of-mind can encourage employee reporting.
- Monitor DNS registrations to ensure that domains are not being registered and MX servers established for sites that may be fraudulently representing themselves to your employees or customers.

[5] Paul Ducklin, *Coronavirus warning spreads computer virus*, Naked Security (2020), https://nakedsecurity.sophos.com/2020/03/05/coronavirus-warning-spreads-computer-virus/

[6] Fleming Shi, *Threat Spotlight: Coronavirus-Related Phishing*, Barracuda.com (2020), https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

Identifying Critical Data Leaks

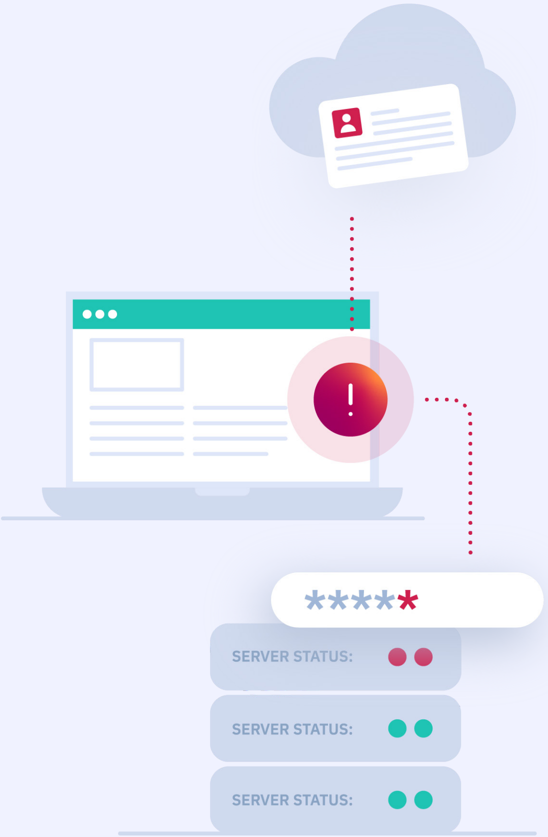
Even with the implementation and enforcement of strong data security measures, negligent data leaks are inevitable for enterprises. Whether through the use of an unapproved tool, a misconfigured cloud account, or falling prey to a phishing attempt, what becomes critical for a company is being able to identify that a data leak has taken place before opportunistic threat actors do. To optimize data leak detection, three elements are essential for your digital risk management strategy.

NO STONE UNTURNED

Overreliance on a single investigation perimeter will leave you with blindspots. The danger of the dark web garners a lot of media attention, but if the digital risk management strategy only addresses the dark web, it is catching the leaks too far downstream when these have already made their way into the hands of threat actors. Detecting data leaks across the entire internet, including the visible web, connected storage devices such as NAS drives, misconfigured cloud storage, and even exposed databases can ensure there are eyes on what has escaped your perimeters.

ADDRESS THE NEED FOR SPEED AND BIG DATA CHALLENGES

In addition to looking everywhere across the internet for potential critical data leaks, it is equally critical to look for everything. The variety of brand marks, products, subsidiaries, domains, and even sensitive project names your organization has is vast and varied. Leaving scans to ad hoc searches is unsustainable and unreliable. When adopting a strategy to identify data leaks, consider one that includes the ability to scale scans to meet your needs, and will leverage machine learning to ensure that the vast volumes of data being collected are processed quickly and effectively.



REMEMBER THE HUMAN TOUCH

As much as technology provides the foundation for your data leak identification strategies, having alerts sent to your security operation teams without context or investigation will prove to overwhelm the team. Automated scans for potential leaks, and a machine learning-powered triage of those findings may result in false positives, which, if sent to your teams will result in lost time and alert fatigue. When assessing a data leak detection strategy, make certain it includes involving an expert analyst to investigate and contextualize automated findings. Ensuring your strategy includes augmented intelligence will ultimately save time and resources in identifying where critical leaks have occurred.

Remediating Critical Data Leaks

Once a critical data leak has been identified, the next mandate for an organization is to remediate that leak. Average time-to-takedown for leaked data is estimated to be 279 days.[7] Each of these days represents an opportunity for a major data breach to be leveraged by a threat actor. Systems can be infiltrated, PII can be published, and important business intelligence exposed or sold. To ensure timely remediation, consider the following when developing your digital risk management strategy.

EXPERT ACTIONABLE GUIDANCE

Much as ensuring a human touch in the identification of data leaks will help you avoid overwhelming your team with false positives, receiving an expert's actionable guidance will help you complete remediation tasks quickly. Beyond a general summary of the leak that occurred, curate a list of all of the information that will be essential for your team to receive from cyber experts in order to execute the data leak management strategy. Ensuring that you receive both context on the source of the leak, as well as step-by-step guidance on how you can have the data secured, will help you achieve the risk and impact reduction benefits you're seeking.

DO-IT-YOURSELF VERSUS DONE-FOR-YOU REMEDIATION

Even with highly-skilled and hard-working security teams with developed policies and tools, the number of data leaks slipping through the cracks unremediated or not remediated quickly enough continues to plague companies across the globe. Resource constraints or surge capacity for your team's bandwidth when a critical incident arises can leave the firm exposed. Establishing a relationship with a vendor offering remediation services is a smart way to either outsource the role entirely or to provide that additional bandwidth when required. Instead of one-off engagements, consider working with a vendor on an ongoing basis, as an extension of your organization with cultivated expertise on your security needs and standard operating procedures.

AN END-TO-END DATA LEAK MANAGEMENT SOLUTION IS KEY

During the first quarter of 2020 the information security community experienced an unprecedented expansion of their organizations' cyber attack surfaces as an increasing number of employees were mandated to work remotely. This rapid wave of change in how employees perform their tasks has meant that legacy security procedures and tools are perhaps unable to maintain the robust coverage required to secure all business sensitive data. Whether revealed via the unauthorized use of shadow IT, accidentally leaked after being uploaded to misconfigured personal data storage devices, or stolen as a result of a phishing campaign, that a firm will experience a data leak is not a matter of *if* but of *when*.

[7] IBM Security and the Ponemon Institute's 2019 Cost of Data Breach Study.

Reduce Your Digital Risk

A data leak management solution is no longer optional in your cybersecurity stack...it is essential.

At CybelAngel, we provide companies augmented intelligence about where their sensitive data has leaked, despite all protections put in place. As corporate ecosystems expand and risk profiles shift, having an increased visibility to where your sensitive data may have escaped corporate perimeters is key to avoiding costly and damaging breaches. CybelAngel's deep and broad scanning of the web, exposed file servers and databases, misconfigured cloud storage and DNS registrations, in combination with machine learning enables us to identify your critical data leaks first and remediate ahead of threat actors.

Please click here to get your free Data Leak Dashboard.

About CybelAngel

CybelAngel reduces global enterprise digital risk by detecting critical data leaks outside the firewall before these leaks become major data breaches. Leveraging its Augmented Intelligence, a unique combination of proven machine learning capabilities and superior cyber analysts, CybelAngel analyzes billions of data sources, thousands of files, and hundreds of threats across all layers of the internet to discover critical data leaks for their customers. Global organizations rely on CybelAngel every day to detect critical data leaks before wreaking havoc on their business.

Learn more at www.cybelangel.com