KONICA MINOLTA

Microsoft 365

INTELLIGENT CONNECTED WORKPLACE

# AVOIDING A CYBER-HOSTAGE CRISIS

**A guide to safeguarding against ransomware and other emerging threats in the new reality of hybrid work.**

## THE BIG PICTURE:

# REMOTE WORK BRINGS NEW OPPORTUNITIES – AND RISKS

**Many small and medium-sized businesses have discovered something during the rapid shift to remote everything: there's a lot to be gained by not relying on a physical space. The move to digital can not only save overhead, but also reduce travel expenses.**

**Some studies have even found that it has increased worker productivity (one saw a 13% performance boost among at-home workers)[1]. As a result, many businesses are considering tools and strategies to make digital a permanent part of their businesses, working towards a hybrid approach.**

This transformation in the way we do business requires new structures and processes, especially for smaller companies not used to working remotely. Regardless of your size, however, all companies now need to revisit their IT security set-up. Employee vigilance as the 'last line of defense' is just as vital as securing all endpoint devices, including frequently overlooked printing infrastructure.
**A recent poll[2] amongst IT decision-makers in the United States shows the extent to which security threats have recently become a widespread challenge for businesses:**

**Over half of the companies surveyed** (54%) name **security and data protection as a major IT challenge**

Similarly, **49%** say they have had a **security breach within their organization's IT in the past two years**

**One in six companies** has experienced a **severe ransomware incident in the past two years**

**35%** attribute **a virus, malware or general security threat** specifically to the **COVID-19 pandemic situation**

1 "Remote Working: The New Normal?" Casey Rue, Forbes, May 20, 2020, https://www.forbes.com/sites/forbestechcouncil/2020/05/20/remote-working-the-new-normal/

2 "The impact of Covid-19 on small and medium sized businesses", Konica Minolta & Keypoint Intelligence Survey, 2021

# DECENTRALIZED WORK MULTIPLIES EXPOSURE TO RISKS

**Like many other companies making digital transformations, your company's first challenge was most likely ensuring unimpeded performance for newly remote workers trying to access their tools and data – or just trying to find a reliable internet connection.**

Your next concern was probably security. Suddenly, strict workplace device policies transformed into bring-your-own-device (BYOD) policies. Almost every employee can now work remotely. They're more likely to be focused on being productive than following your pesky security procedures. They'll access their data however they can, often bypassing VPNs to access cloud services or hopping on to the closest Wi-Fi hotspots – whether they're secure or not. This do-it-yourself approach can lead to risky activities beyond your control, such as employees downloading software without your IT department's knowledge. With everyone using whatever devices are handy – personal phones, home computers, even kids' tablets (it has happened!) – the situation becomes rather dangerous. One wrong click can launch an attack that could jeopardize your entire business.

Given the limited capabilities of traditional perimeter firewall and VPN solutions to protect against remote threats, companies need new security measures, levels of expertise, and technologies to protect their assets. The good news is that you can build on existing measures and solutions to achieve a higher level of security.

## TIME IS NOT ON YOUR SIDE:

# GET A HANDLE ON YOUR SECURITY PICTURE

If you haven't had time to perform basic endpoint hygiene and connectivity performance checks on your computers and endpoint devices, it's better late than never. In addition to confirming your laptops (and printers!) have the necessary endpoint protection configurations, ensure your employees are following recommended security practices by asking the person in charge of IT these three important questions:

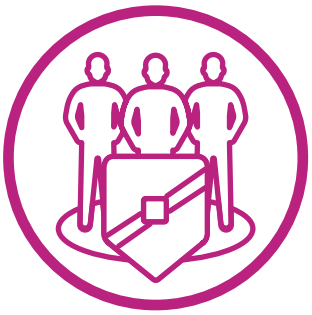
**1.**

**Have we reviewed and adjusted the security settings of our cloud access points as well as our organization's internal network?**

**2.**

**Have we ensured that the security settings and measures for remote users are appropriate for current and foreseeable levels of usage?**

**3.**



**Is our team – including both users and IT staff – aware of all the latest security threats or do they need further education?**

# YOUR DISTRIBUTED WORKERS ARE YOUR ALLIES IN PROTECTING YOUR IT

**Remote workers are no longer the outliers. Their devices can no longer exist at the fringes of your security plan; they are dead center and must be treated as such. The mixing of company and personal devices demands separate practices and elevated levels of control. This means much more than the basic antivirus and antispyware protection; it means multi-factor authentication (MFA) and onboard endpoint detection and response (EDR) capabilities.**

Your remote workers should not only be aware of these new measures, but the tools and safeguards you use to attain and remain at a new level of endpoint and data security by deploying them. With the world rapidly – and permanently – changing, now is the time to partner with a solutions provider that lives and breathes security best practices.

Without this critical help, you can't be sure each endpoint meets security policy requirements. You need the right tools to track and enforce policy on all devices and with employees everywhere, while delivering easy user onboarding and offboarding.

**WE CAN HELP.**

# YOU HAVE ENDPOINT DEFENSES. BUT ARE THEY ENOUGH?

Gold Microsoft Partner

**The decentralization of the workplace makes endpoint security more critical than ever, especially as threats are likely to target a breadth of opportunities, potential vulnerabilities and even place previously unthought-about devices such as printers and MFPs also in the crosshairs. The new tactics used by malicious actors require focus across a spectrum of different tools and solutions.**

If your organization uses Windows 10 or later, odds are that you already have access to a world-class anti-virus and anti-malware solution built into the operating system. You also probably have the cloud license to activate tools with centralized management and greater capabilities.

Microsoft provides unmatched breach remediation and research capabilities. You can enable your security team to graphically map the precise point at which an attacker entered your network, how they moved, and the activities they engaged in once inside.

It is one thing to remediate a network breach but having the rich details of exactly how it occurred enables you to make sure any vulnerabilities in the network are found and corrected to make sure the breach never happens again.

Yet, these measures will not prevent hackers from persisting – instead better defense in general inspires ever more sophisticated lines of attack, including targeting endpoint devices such as printers. In fact, ransomware attacks have significantly grown more sophisticated in the last few years, causing ever more damage to organizations. In the past two years alone, 16.5% of firms surveyed by Konica Minolta experienced a severe ransomware incident and twice as many (35%) experienced at least one "less severe" incident[3].

**Considering the significance of this threat, let's talk about how ransomware works, and what you can do to stop it.**


3 "The impact of Covid-19 on small and medium sized businesses", Konica Minolta & Keypoint Intelligence Survey, 2021, https://www.konicaminolta.eu/eu-en/news/konica-minolta-research-reveals-the-impact-of-covid-19-on-small-and-medium-sized-businesses

# RANSOMWARE 101:
# HOW THEY GET YOU

**As its name implies, ransomware takes your data hostage through encryption – preventing you from accessing it. Here's how the typical ransomware attack develops:**

### 1. ACCESS

Most ransomware arrives through phishing emails – messages designed to trick someone into entering their credentials or interacting with malicious content. It could be an Excel file with macros that release ransomware when enabled, a hidden executable file, or a link to a malicious or fake website.

### 2. INFECTION

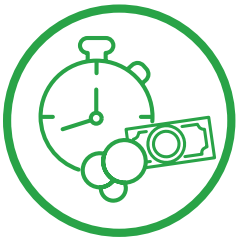
Once released, the virus installs itself on the targeted machine and attempts to gain access to any data, resource, or system it can on your network. This includes access to keys to your network, important documents, or even built-in security measures that could impede the virus' progress.

### 3. SPREAD

Ransomware is designed to spread. It infects any machine it can. It will find out as much information as it can about your infrastructure. It will identify and spread to network shares, smart devices, and other resources it can access.

### 4. ENCRYPTION

Once the virus has spread and gained access to a significant part of your infrastructure, it will "activate" and encrypt all the files it has access to. This is usually the first time you realize there is an issue.



### 5. DEMAND

After compromising and encrypting, the virus then sends its victims a message making a ransom demand. This could be an ask for payment with a promise to release and return all the files, a warning that sensitive information will be published online, or a threat to sell data on the dark web. In a frightened panic, victims often pay the ransom. Instead of solving the problem, the payment encourages more cybercrime and provides no guarantee that the criminal will release the hijacked data.

**Although the consequences of ransomware are drastic, there are ways to prevent these attacks and minimize your loss.**

# FOUR WAYS TO LOWER YOUR RANSOMWARE RISK

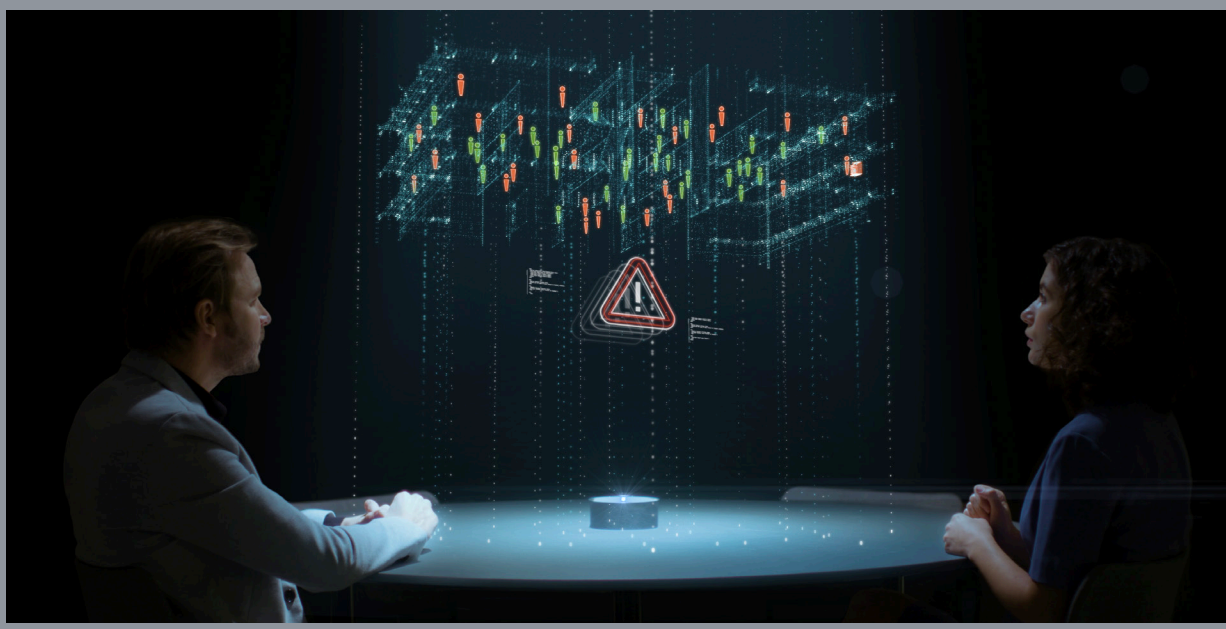
## 1. ENDPOINT SECURITY: BE PROTECTED FROM THREATS ENTERING IN THE FIRST PLACE

Securing your organization's IT is the first line of defense – any threat blocked from entering the organization in the first place is a bullet dodged. While organizations have already amped up security to protect computers, servers and mobile devices, other endpoint devices such as printers are frequently left unprotected. Yet, they can be misused as an entry point by hackers. By exploiting a security vulnerability in a connected device, a skilled hacker can expose an entire network to data theft or disrupt business processes and cause significant costs with a targeted ransomware attack.

To protect its customers, Konica Minolta puts its products through rigorous internal cybersecurity tests and ensures they meet PCI, HIPAA, FERPA and GDPR compliance requirements. But to further assure customers that the printers exceed industry standards for cybersecurity compliance, Konica Minolta invested in an extra layer of threat protection: penetration tests provided by NTT DATA and the Security division of NTT Ltd. After 80 hours of hacking attempts, no vulnerabilities were found in the penetration tests recently conducted on the bizhub i-Series.

Konica Minolta further provides its clients with a Bitdefender Antivirus i-Option Bitdefender scans incoming and outgoing data in real time for infected data. If, for example, print jobs are infected, Bitdefender deletes them.

Furthermore, the bizhub i-Series can be equipped with bizhub SECURE, a special offering for MFPs on which different security levels can be set to ensure the security of office devices and protect device memory and network settings. A notifier app also warns the responsible project owner when settings are changed.



## 2. Phishing: Be the one that got away

Ransomware depends on social engineering to succeed. According to Secureworks, half of all internet users receive at least one phishing email per day – and 4% of them click on them. They also found that phishing attacks are up by 667% since early 2020.[4]

Once inside a network, hackers can completely mirror the emails of legitimate internal users. When a user receives an infected message and clicks on the included link, the ransomware is deployed.

While securing endpoints is the first line of defense against such attacks, employees themselves represent the last line of defense when it comes to security. We can help ensure your employees follow security best practices to help keep your business safe.

## 3. Be aware of unsanctioned apps

The new hybrid world of work is full of smart end users, who are bound to think they have better tools than those of your IT department. Sometimes a tool can go viral, becoming the app-of-choice before IT can stop it or even become aware of its existence.

Though your users may see these as smart and cool new solutions, they're dangerous to your data security and can become the source of network breaches. How? The provider of the app may have inferior security standards and have been breached. In fact, downloading an infected app is the most common way for Android devices to become infected. Even worse is the prospect of Ransomware 2.0 that infects cloud software-as-a-service providers. [5]

## 4. Be ready to recover

Given that last year 50% of businesses experienced unforeseen interruptions and of those, 81% resulted in business closures of a day or longer, the necessity of a data backup and recovery plan is obvious. A properly designed and tested disaster recovery (DR) plan can be the difference-maker in your thriving business surviving a catastrophic loss of your critical systems.

While you can develop a DR plan on your own, the best and most cost-effective course for a small or medium-sized business is to work with a solutions provider. These companies have a proven track record building, managing, and testing DR plans for businesses like yours.


4 "Cybersecurity Awareness Training: Threats and Best Practises", Secureworks Blog, November 12, 2018, https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices

5 "The Future of Ransomware 2.0 Attacks", Dmitry Dontov, Forbes, June 5, 2020, https://www.forbes.com/sites/forbesbusinesscouncil/2020/06/05/the-future-of-ransomware-2-0-attacks/?sh=33a331d04dc9

## CASE STUDY

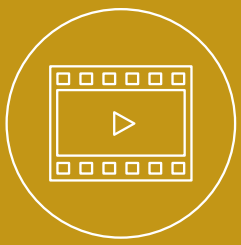
# ONE CREDIT UNION'S SUCCESSFUL SECURITY JOURNEY

**WHO: JM Associates Federal Credit Union**

**WHAT: Credit Union, Financial Institution**

**WHERE: 5 offices- 2 in Jacksonville, FL, and 1each in Deerfield Beach, FL; Mobile, AL; St. Louis, MO**

**SIZE: Serves over 8,000 members**



Following a routine information security examination, JMAFCU learned they needed assistance improving their cyber security posture. Average security for a credit union with members who rely heavily on them to secure their financial information was not up to the standards the board and executive management believed their members deserved - JMAFCU wanted to improve to the maximum level, the most secure. JMAFCU's leadership decided to do whatever was necessary to achieve a higher rating to improve service to their members.

Fairly common for a single SEG credit union, JMAFCU relied heavily on their sponsors' network security and network provisioning systems. While this method saved time and money, it also afforded JMAFCU less visibility or control over their own security measures. After the examination brought to light some areas of security where the credit union required more documentation, segregation and visibility, President Jim Ryan realized the credit union may need to seek an alternative means to maintain and enhance their security landscape. When JMAFCU realized they didn't have the resources to address these challenges alone, they turned to All Covered, the IT Services Division of Konica Minolta Business Solutions USA.

Upon learning about the information security initiatives at JMAFCU, All Covered's Dave McOlgan, Information Security Consultant, offered the credit union a full service Baseline Information Security Assessment. Not only did the assessment highlight opportunities for enhanced security, it also showed other areas within the organization that could be strengthened, such as policies and procedures, report reviews, and vendor management.

Once the assessment was finalized and shared with JMAFCU's Information Security Committee, questions arose as to how to best implement changes to enhance security practices in the most efficient way. All Covered was able to create and implement a custom security and compliance plan for JMAFCU that would work with their business needs and show them how to be more proactive in mitigating cybersecurity risks, all while keeping costs manageable.

The baseline assessment was the initial step in building out the roadmap of success for JMAFCU. All Covered was able to collaborate with Jim Ryan, President, and Paul Numbers, JMAFCU's Chief Financial Officer, on executable processes and programs and create a timeline to track milestones along the way. The plan is still in progress today.

Throughout the roadmap, the team has also been proactive in changing and evolving systems and processes to ensure a secure organization for associates and members. One important component is cybersecurity awareness training for associates. The President, Jim Ryan, has even mandated cybersecurity tests via email that are routinely given to employees at random to ensure they are treating information and data in the most sensitive and ecure way. "We want our members as well as associates to feel comfortable that their data is fully secure and cannot [easily] be compromised, it's why we believe in continuous testing, training and results; what gets measured, gets done."

# BRING A TRUSTED PARTNER ON BOARD FOR 360º SECURITY

## HELPING YOU FEEL SAFE

IT environments gets more complex every day. No matter what type of business, you are at risk of system penetration from external forces such as hackers as well as leaks, losses and threats from malware.

We understand that one technology alone cannot offer enough protection against cybercrime and other security threats. This is why Konica Minolta has years of experience building a broader approach to IT security: today, we bring you a complete service built around a comprehensive information security concept that spans people, processes and technology.

Konica Minolta's 360º security view considers all the elements of your business: your people and the digital technology and processes they use each day. Konica Minolta's information security concept starts with the premise that comprehensive information security is only possible if areas such as IT security, data security, the protection of multifunctional systems and printers and the security of any video security systems as well as building and perimeter protection are considered together.

Using this 360-degree approach, Konica Minolta creates a customized solution for our customers that meets their security needs and avoids additional effort and cost. Our team brings you the benefit of over 25 years of experience and can develop a strategic approach to your security. We'll make sure we add value and give you a transparent and sustainable service with fast response times.

## EMBRACE THE OPPORTUNITIES OF DIGITALIZATION

Modern IT offers great potential for companies. While small and medium-sized enterprises often lack the resources to keep a constant eye on the complexity of their infrastructure and potential weaknesses, a strong partner like Konica Minolta can empower you to tap this potential safely with well thought-out, comprehensive security strategy. Find out more about how we can help protect your organization here: **http://kmbs.konicaminolta.us/security**

**KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.**
100 Williams Drive, Ramsey, New Jersey 07446

**ReshapeWork.com**

09/21-P