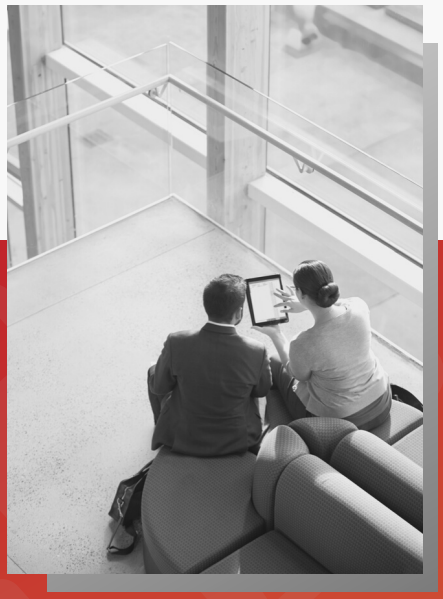
MicroAge®

The Digital Transformation Experts



The Essential **Ransomware** Security Guide

Everything you need to know to arm your organization *against digital disruption*

microage.com

(800) - 544 - 8877

Table of CONTENTS

MicroAge®
The Digital Transformation Experts

Fuel smarter business outcomes and connect your workforce with MicroAge.

THECHANNELCO.
CRN®

MicroAge has been awarded:
- Top MSP 500 - Elite 150
- Top Tech Elite 250
- Top Solution Provider 500

Proactively building out an IT security strategy is mission-critical to protecting your business and remaining competitive.

Ransomware attacks are on fire—we have some shocking stats to prove it. Organizations of every size are under attack, including local governments. According to the Baltimore Sun, the Baltimore City government lost over $18 million and had challenges for over a month in getting back to "business as usual". According to Comparitech, last year's ransomware damages were predicted to pass $8 billion and were up 12%. And ransomware downtime costs most organizations over $64,000, while these attacks are costing businesses across the enterprise over $75 billion every year.

Approaches to securing the remote workforce are changing daily with new threats coming into focus including new COVID-19 malware. Hackers are even crashing confidential conference calls, targeting the growing number of companies using conferencing tools like Zoom.

Having the right security strategy has never been more important to your organization.

The stakes were already high, with an OFAC advisory that came earlier in the year, warning business IT leaders that their organizations can be fined and sanctioned for paying ransomware hackers identified as cyber terrorists by the United States and its allies. Since then, the cybersecurity threat has plagued governments and business communities in a much more visible way.

Don't be the next national ransomware headline.

In case you've been avoiding the news, now is a critical time to ask if your organization is armed against ransomware attacks. Because while ransomware survival isn't a new challenge for technology leaders, it's a national security topic that is dominating global news and government agendas.

The Colonial Pipeline and JBS hackings are a stark cautionary tale on the importance of factoring security into your disaster recovery strategy. And it isn't just government officials and news anchors talking about ransomware, it's become a national topic with growing consumer visibility as the nation braces for potential cost increases and shortages of everyday necessities.

Ransomware sparked a national dialogue in 2020 after a Russian hacking group bypassed multi-factor authentication and rocked the international business community with the SolarWinds cyberattack.

The Deputy National Security Advisor pinpointed one of the main factors driving the increase in ransomware attacks. "The misuse of cryptocurrency is a massive enabler here," explained Deputy National Security Advisor Anne Neuberger. "That's the way folks get the money out of it. On the rise of anonymity and enhancing cryptocurrencies, the rise of mixer services that essentially launder funds."

> ***"Individual companies feel under pressure—particularly if they haven't done the cybersecurity work—to pay off the ransom and move on," Neuberger added. "But in the long-term, that's what drives the ongoing ransom [attacks]. The more [ransomware hackers] get paid the more it drives bigger and bigger ransoms and more and more potential disruption."***

That's key, and Neuberger highlighted a critical factor here: organizations who haven't done the cybersecurity work feel the pressure under attack.

Stop the digital extortion machine

Successful ransomware attacks are penetrating the U.S. business enterprise and economy with devastating consequences, and the FBI anticipates a continued surge. But there's good news, preventing a ransomware attack doesn't have to be difficult. If securing your organization wasn't your priority before it should be now. Because you don't want your organization to be the next news story like the leading beef supplier who paid an eye-popping $11M in ransom. Costs that economists are speculating could be passed onto consumers directly.

And while cyberattacks against the American enterprise increased by 80% in 2020 with phishing attempts jumping by 600%, the Biden administration is preparing for a massive increase to come.

While the FBI and other agencies are hard at work to prevent further cyber-attacks felt across the country, there is no silver bullet when it against ransomware attacks. There is no shortcut to doing the cybersecurity work because prevention is the only concrete solution. Having a solid backup and security strategy can guard your organization and your customers against becoming a statistic, making your data accessible in seconds or moments to avoid far-reaching economic consequences that can damage a company's image forever.

In this eBook, we review how you can act to prevent ransomware attacks from disrupting your business.

Educate your workforce.

This might sound like a no-brainer, but as you can see from the example before, just one employee clicking content from the wrong email can compromise your entire organization. Ransomware can start with an email or SMSishing attempt, so arming your employees is an important first step.

It's important to create a security training program to prepare your workforce to see the signs before a cyberattack occurs. That means running an effective security compliance training because spam filters aren't enough. Employees need to be trained on the latest policies and the basics for recognizing suspicious content and scams. It isn't a one-and-done training—repetition is everything to get your team members thinking before they click anything.

You can get some great feedback from your associates too. Ask employees what they are seeing and deleting and ask them to report anything suspicious to IT so you can prevent their colleagues from getting trapped. Here are some basics every business should use to arm their organization and their workforce.

Safeguard with 4 steps

01 step — Run an effective security and compliance training

02 step — Test employees with simulated phishing campaigns

03 step — Implement your work security strategy

04 step — Keep an active dialogue going with your team members

1. Run an effective security and compliance training

Thinking spam filters will keep the company safe, employees are frequently lulled into a false sense of security. They should not only be trained on policies and protocol to follow, but also basics on how to recognize a scam, why strong passwords that change regularly are necessary and the types of personal information they should avoid sharing with anyone.

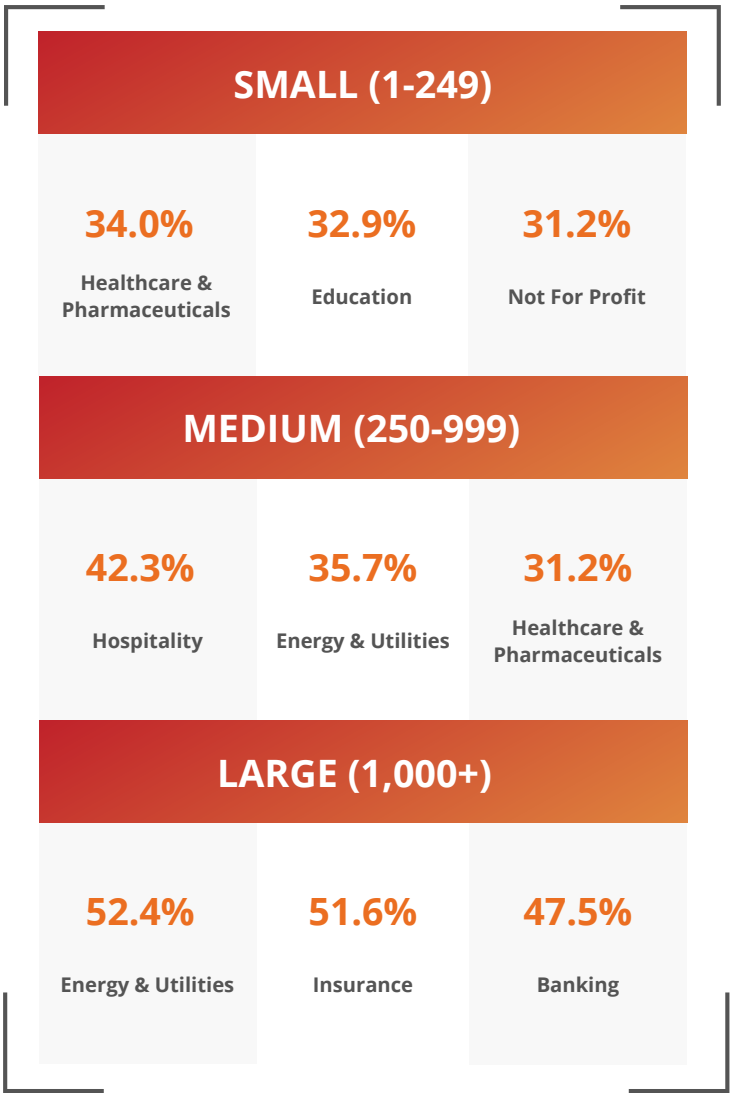
Make the training mandatory and explain the newest threats to your team and how to counter them with basics like VPN, using their Single Sign-On (SSO), and reporting any emails to your IT team that don't look right. Why? Spam filters aren't catching everything. In fact, spear phishing messages have an open rate 5-6x higher than actual marketing emails—70% of employees fall for them.

And that number is increasing with more people working remote in social isolation and more receptive to communications from people they don't know. Your virtual training should also highlight SMSishing—these attacks via text can become more common with more people looking to connect and current events. Your team members should be on the lookout for suspicious text messages on subscription services they haven't heard of previously or warranties coming to an end.

2. Test employees with simulated phishing campaigns

Sound extreme? It isn't when you look at the statistics below. To determine what details employees provide that they shouldn't, send simulated messages to see how they react. This immediately identifies areas where additional training is required. Training that should be followed by another simulation to gauge progress accurately.

Top 3 Industries at Most Risk by Organization Size



3. Implement your remote work strategy

Cyberattacks and social engineering are powerful tools because too many employees aren't on guard or aware of the importance of data security—even more than usual when they're dealing with stressors outside of work. It's critical to educate your team members on how you are securing them and the business and on the role they play.

Build or finetune your Cybersecurity policy for remote workers. Explain why you're introducing the policy—the kinds of new emerging threats—and how they can keep the business secure while they work from home. Guide your teams through the high-level details before sending the strategy out to all employees to review and sign.

When you create your policy, make sure you start it with a mission statement, (the why), and then distill it to the specifics on security policies across all devices—personal and company-owned.

After launching your security policy, keep reinforcing why compliance is critical and how you're supporting compliance with tech, coaching, and other resources with regular communications.

4. Keep an active dialogue going with your team members

You can get some of your best intel from your own team members. Ask your employees what they are seeing, and what they are deleting. Encourage them to report any suspicious messages to prevent their colleagues from falling prey.

Most of our team's clients are absolutely shocked at what manages to get through their defenses. Our experts at MicroAge have helped their biggest stakeholders see the need for teaching employees to be a human firewall.

Get clarity on back up versus archiving

Data archiving is the long-term process of storing and retaining data. Data that's archived often isn't currently in use, but it can be restored in the future as needed. For example, your organization probably keeps an active archive of dated email interchanges handy in case of organizational shifts, changes in personnel, or fresh legal matters. It's a lot like putting your not-so-relevant data on ice in case it becomes relevant later.

Alternatively, data backup is defined as the process of duplicating data for retrieval in case of a data loss event. Backing up data makes a second set of all your files (current and dated) so you can restore them later in the event of a natural disaster or cyber-attack. Everyone needs a backup, that's especially true for any organization because of the value of data. After all, in recent years data's worth surpassed that of oil.

Here are the major differences between archive and backup that you need to understand:

Preservation isn't recovery

Archiving and backing up data have very different purposes and capabilities. The most important distinction is that archiving is dedicated to long-term data preservation and retention while backup is all about recovery in the event of an emergency. Archiving preserves the files you want to keep on hand while backing up protects your business so you can restore everything

---

Access levels are different

Because they serve different technical functions, backup and archive applications offer different levels of user access. Archives are built to put those individual files like word documents, databases, and email messages on ice so they're easy to locate later. When files are archived, their metadata is also, making it easy to find that email Bob sent you about best practices two years after his retirement party. Archives aren't meant to be used for a total recovery.

Meanwhile, backup data is generally there for backup in case you need a large-scale recovery later. Backup applications are used for data objects and individual files, but they're intended for significant recovery efforts—recovering files, systems, and applications.

Disaster recovery is key

You're probably noticing a trend when it comes to what makes backup so different—it's all about preparing for disaster recovery. That's because backup is integral to Disaster Recovery (DR). When you're backing information up, you're protecting that data offsite—usually on the Cloud—in case of a disaster. Archiving maintains your archive system, but it won't save your data in the event of an emergency.

That's important to remember because the number of annual ransomware attacks doubled this year. These attacks have been costing businesses and even local city governments millions to retrieve stolen data from hackers or rebuild their systems.

Backup locally and on the cloud.

Backing up your data and system can prevent damages that you cannot recover from and can keep you from getting trapped paying a ransom in the future. And even if you're keeping an active archive of your data and files in place already, that's not enough. Backup is mission critical to disaster recovery of any kind—especially after a natural disaster or a cyberattack—because archives help with preservation, not recovery.

In the event of a ransomware cyberattack, restoring your files from a secure backup is the fastest way to regain access to your data and systems. Cloud backup solutions are ideal for protecting your data, so it isn't infected by ransomware. This backup is an extra layer of production every organization needs.

Run regular security scans and assessments.

Frequently running scheduled security scans is mission-critical. Security software can't defend your system if you aren't running scans across all your organization's data frequently. But just running those scans isn't enough.

At minimum, make sure your IT department is performing an annual security assessment to see where your vulnerabilities are and spot them before they can compromise your organization. Having the right security partner can change everything for small to medium businesses that are frequently targeted without having an abundance of IT personnel or resources. Bringing in outside experts can support better anti-malware and ransomware software, comprehensive training, and a stronger security strategy overall.

Keep your systems up to date.

Making sure all your software is up to date with necessary patches can keep your organization more secure. Malware spread by exploit kits on websites that have been compromised target vulnerabilities with more dated software. To prevent infection, regular patching and updates are a must.

Secure SaaS applications.

Cybercriminals know that the enterprise and other businesses are moving workloads and data to the cloud in a mass exodus from the traditional data center. This started in recent years with more organizations looking to harness greater agility for a competitive edge, and only increased in 2020 with businesses needing to quickly support a remote workforce for the health of their employees and their business operations.

So, it isn't a shocker that SaaS environments have become a big, red target for bad actors. Cybercriminals know that IT teams are even more burdened than business-as-usual with management of SaaS applications and their organization's cloud strategy and footprint, and they see that as a powerful vulnerability to exploit.

Tools for scanning APIs between applications to automate SaaS configuration while monitoring user access and activity and changes in the environment are becoming more important every day.

80%

of workers admit to using SaaS applications at work without getting approval from IT

How to assess your ransomware preparedness?

The NIST Cybersecurity Framework has become the industry standard for gauging how integrated cybersecurity risk decisions are factored into big-picture business operations. It uses four tiers to measure cybersecurity risk: partial, risk-informed, repeatable, and adaptable.

A security assessment can help your organization quickly pinpoint risk factors and act to prevent them from becoming national news. Because ransomware attacks cost the enterprise $8B every year, and every dollar spent was preventable.

We can help.

MicroAge navigates security assessments measuring cybersecurity risk management effectiveness using these five functional areas of the NIST Cybersecurity Framework to gauge how integrated cybersecurity risk decisions are factored into broader business operations:

This three-part, 45-minute maturity assessment dialogue quickly identifies security gaps and enables your organization to:

- ☑ Assess your unique data value to threat actors by factoring in your business function, size, industry, and stakeholders with a Threat Profile
- ☑ Examine your ability to identify, protect, detect, respond, and recover to maintain security leveraging a Maturity Profile
- ☑ Gain clarity around your current approach with a security maturity grade (A, B, C, or D), detailed results, and recommended next steps

MicroAge covers all your security needs, including:

- Security Strategy
- Policy and Procedure Development & Management
- Network Behavior Anomaly Detection
- Host Intrusion Detection and File Integrity Monitoring
- Managed Security Services
- Application Security Testing
- Compliance & Regulatory Standards
- Physical Security
- Social Engineering

Scale your security and your business.

Start building your security strategy. Call your MicroAge account executive at (800) 344-8877 or visit MicroAge.com to get started.