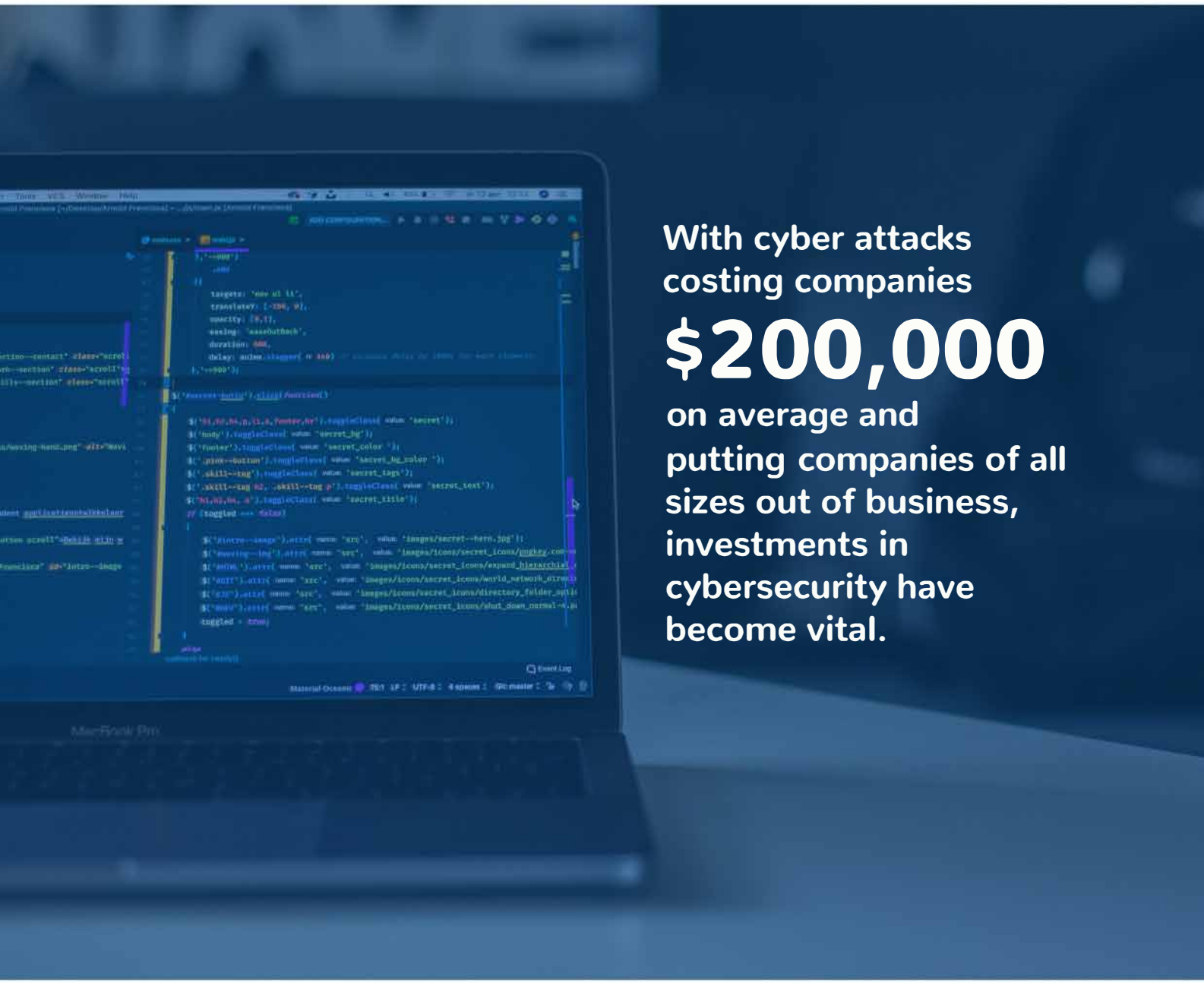
Ntiva

Managed IT, Security, & Cloud Services

MY BUSINESS IS DOING EVERYTHING POSSIBLE TO PREVENT A CYBER ATTACK

E-book: The Must Have List for Cybersecurity Protection

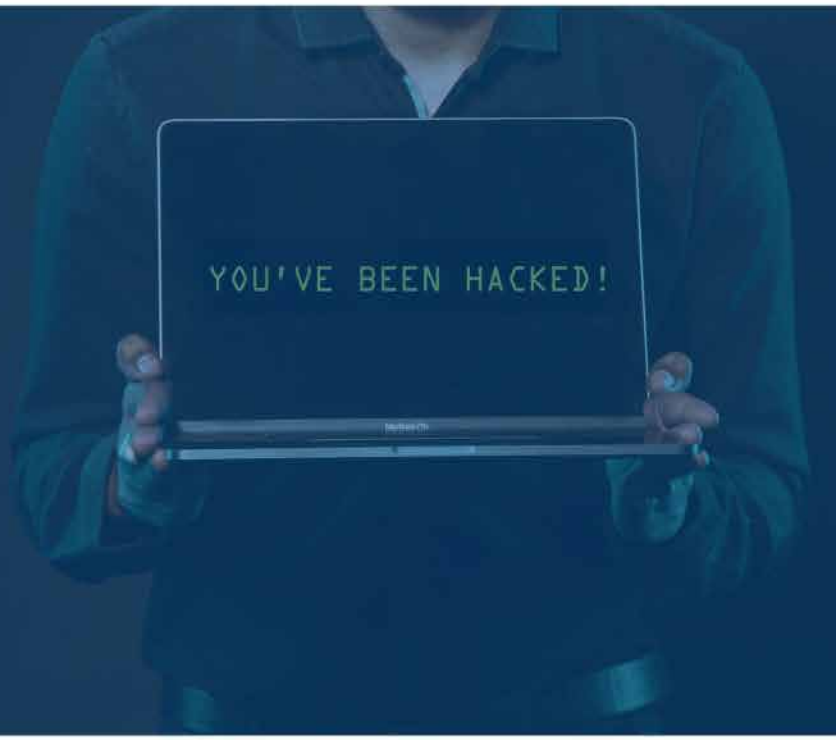
7900 Westpark Drive, Suite A100 | McLean, VA 22102
1-888-996-8482 | www.ntiva.com



Small and mid-sized businesses are far from immune and have become favorite targets for attackers because they are easier to penetrate and lack security expertise.

Whether your implementing a security strategy yourself or auditing your security talent, here are some cybersecurity must-haves to protect your business regardless of size.

Here is your must-have list for cyber protection:



01 PROCESSES & SOLUTIONS

☐ Keep Technology Assets Updated

Everything from your network routers to your PCs to the applications on your phone needs constant updates to the latest versions to protect against ongoing security threats. Update these assets automatically whenever possible.

☐ Install Anti-virus Software

Although far from a comprehensive security answer, anti-virus software is still a basic must-have for businesses of all sizes. Ensure anti-virus software is installed on every device and automatically updated.

☐ Guard Physical Devices & Records

Keep in mind cyber security threats can start offline. Automate screen locks, update passwords, encrypt sensitive data, and keep physical records secure and monitored.

☐ Require Multi-Factor Authentication

It only takes one vulnerable password to allow attackers access to your entire business network and data, whether the password is to Office 365 or Salesforce.com. Protect your on-line applications with a business-wide **Multi-Factor Authentication (MFA)** requirement.

☐ Minimize Administrator Privileges

Do not let workstations run in administrator mode or provide more access than is needed to software and other technology assets. Excess access rights expose your business to more

☐ Enable Email Encryption

Choose a standardized tool that allows for the secure sending and receiving of sensitive files and train staff to use encrypted email for confidential data.

☐ Screen Potential Employees & Contractor

Firms should do a thorough background check on all potential employees and contractors before allowing access to valuable resources. Proactively audit and remove access once no longer required.

☐ Set Automatic Backups and Encryption of Data

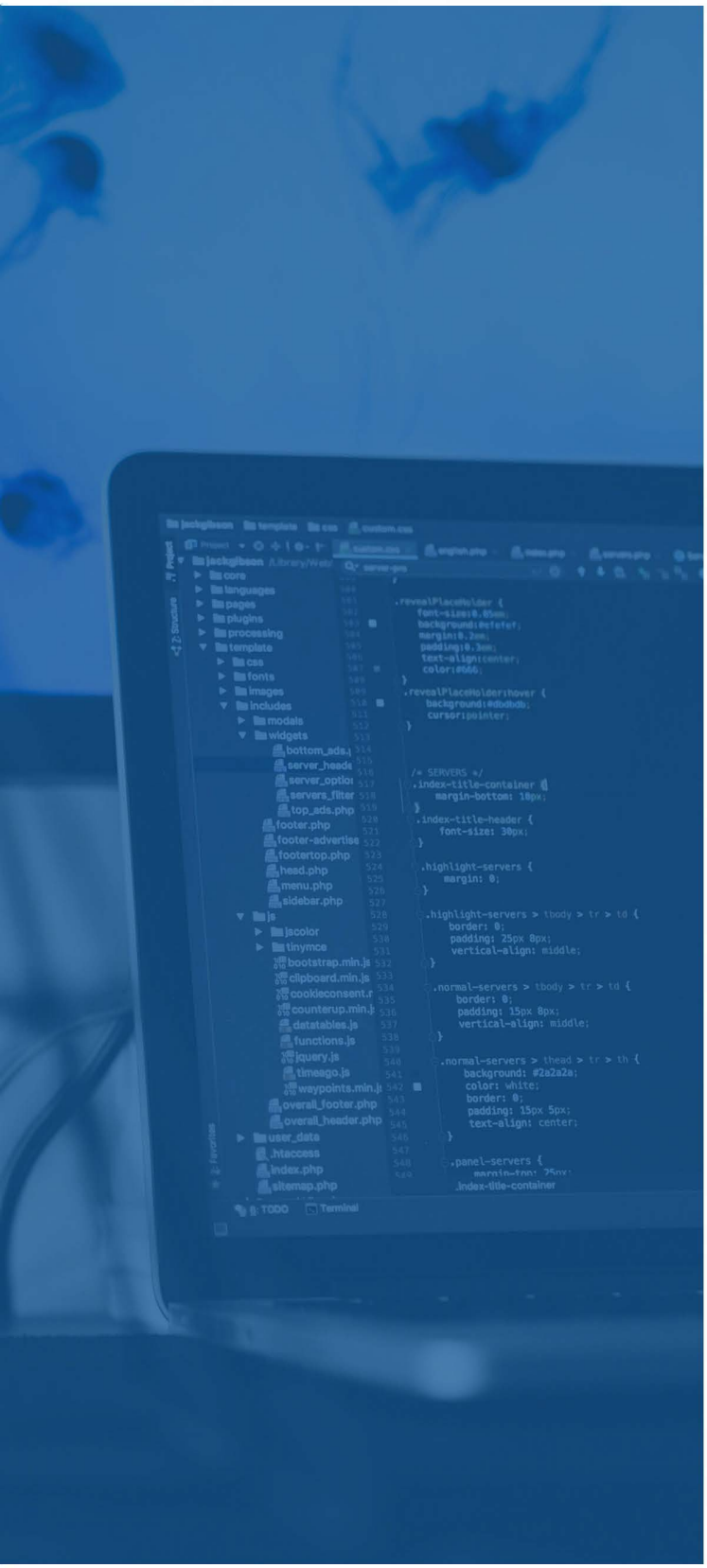
Backup media, such as laptops, that leave the office and validate that the backup is complete and usable. Regularly review backup logs for completion and restore files randomly to ensure they will work when needed.

☐ Eliminate Outdated Hardware and Software

Eliminating outdated hardware and software via server consolidation and virtualization not only dramatically lowers maintenance costs but also reduces your exposure to attacks.

☐ Get Cybersecurity Insurance

Unfortunately, firms can do all the right things regarding security and still fall victim to a cyber-attack. Cybersecurity insurance is now economical and a necessity for most businesses.



STRATEGY 02 & PLANNING

☐ Create & Document a Backup and Data Recovery (BDR) Plan

Despite your best efforts, the chance of a data breach in today's world is extremely high. Be sure you have a **BDR plan** in place and review annually as technology evolves.

☐ Create & Document a Business Continuity Program

Different from BDR, a **business continuity program** documents how your organization will respond to, continue through, and provide normal levels of service despite severe disruptions. Many firms must have a BDR plan in place to meet industry regulations.

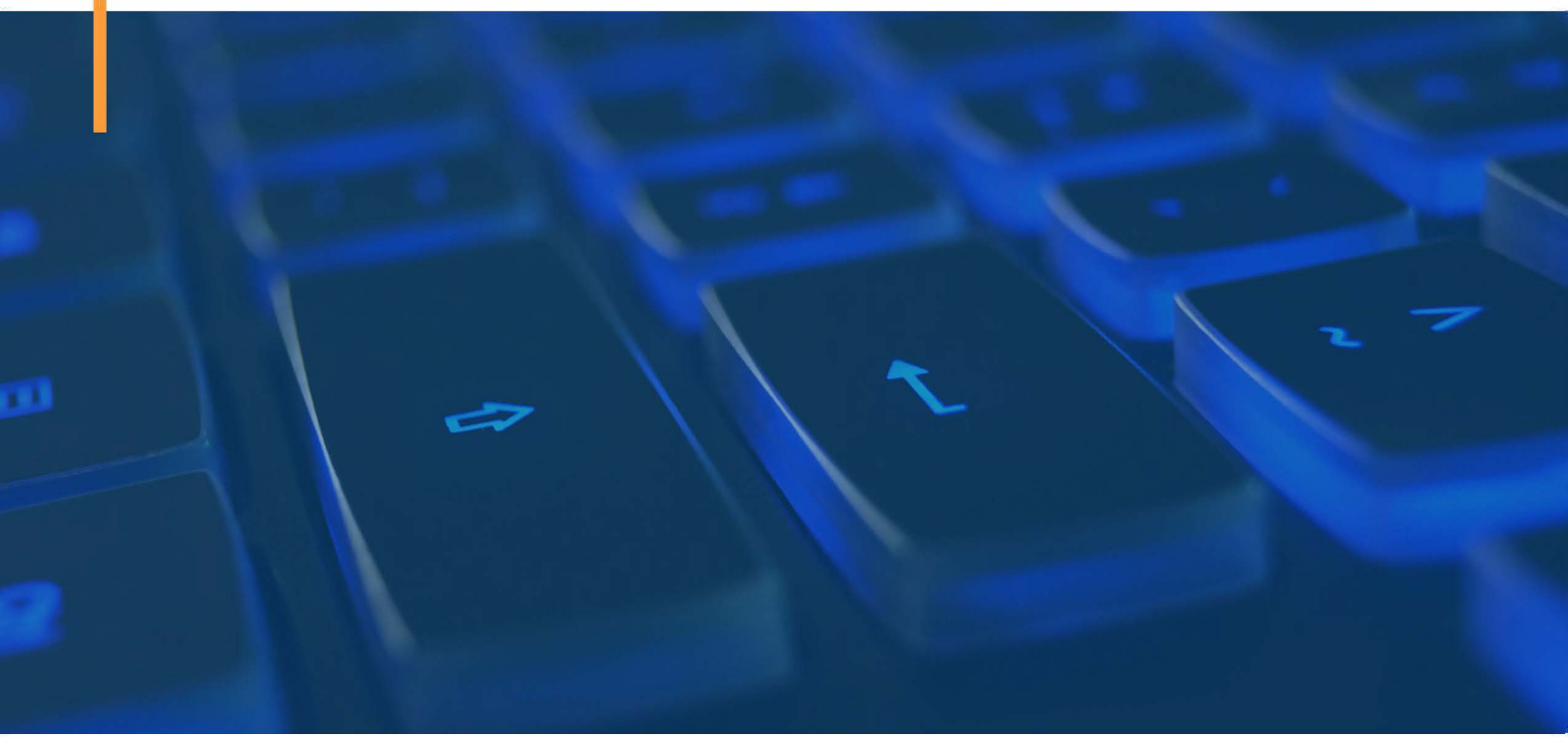
☐ Create & Document a Breach Response Plan

Have a formal security incident response plan in place in the event your data has been compromised, including an internal and external communications plan.

☐ Outsource or Hire an Information Security Expert

Many small businesses have challenges affording and finding an experienced information security expert yet need critical assistance to develop and implement security policies, technology, and threats as they evolve. For a certain number of hours per month, you can tap into outsourced **senior security experts** who can advise you on your business security plan and critical investments.

PROACTIVE SCANS & AUDITS 03



☐ Perform Routine Security Audits

Every organization needs to perform an annual audit as the cybersecurity landscape is constantly changing – and in some industries, your business may require an external auditor to certify your compliance.

☐ Audit Your Data Locations and Access

Keep updated accounts of all your data locations, including servers, workstations, mobile devices, thumb drives, backup systems, and cloud locations – and limit who has access. When possible, have a security expert audit for vulnerabilities and proactively remove access and shared links for those who no longer need it.

☐ Create a Device and Software Inventory

Creating **a hardware and software inventory** helps you know what your business needs to protect and who has access.

☐ Follow & Audit for Industry Compliance Standards

Most industries today require specific privacy and compliance standards for customer data security and more. Consider hiring or **outsourcing an expert to remain compliant** as standards, technology, and threats evolve.

☐ Automate Comprehensive Vulnerability Scans

Regularly **scan your network** for vulnerabilities attackers are most likely to target. These can include missing security patches, insecure settings, or unneeded service. Be sure to prioritize remediating any findings from your scans before threats occur.

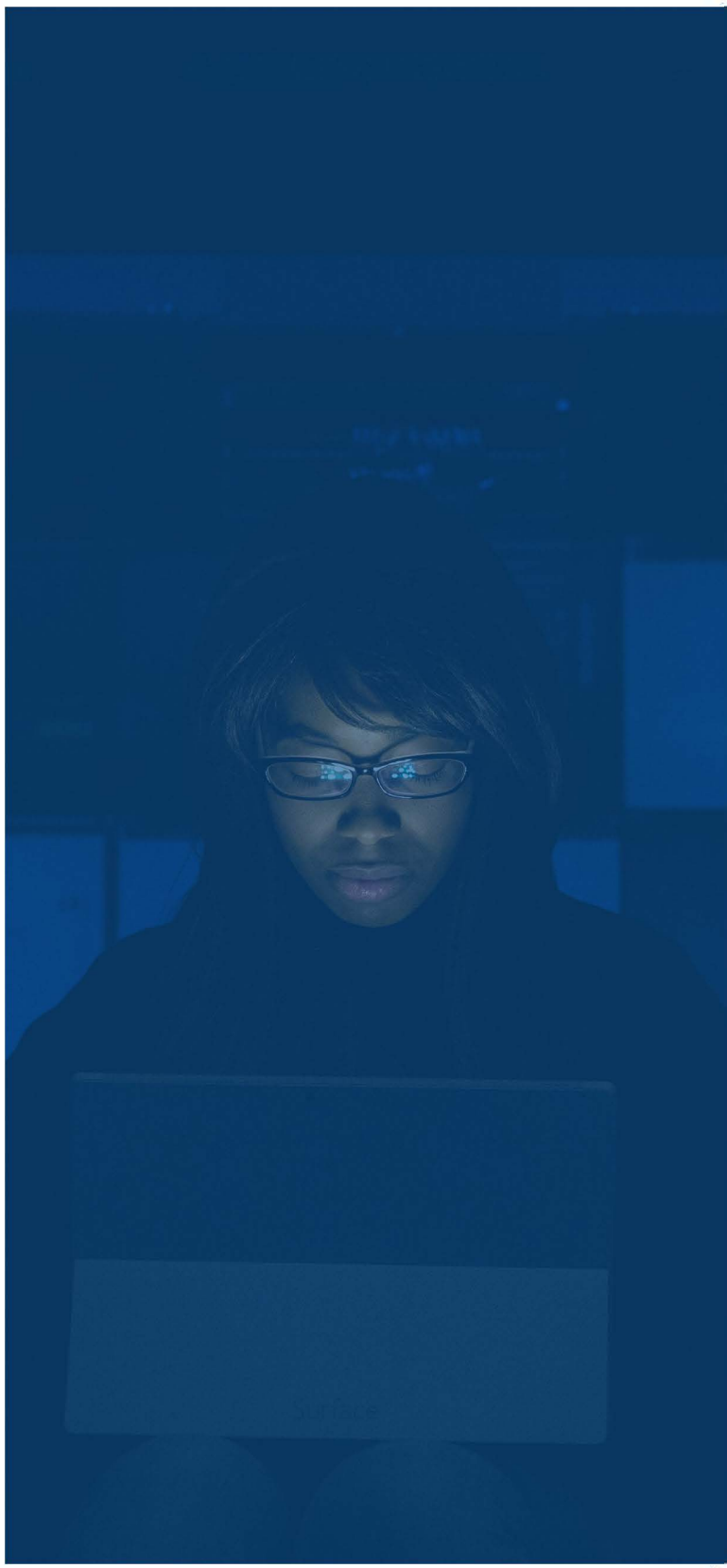
☐ Leverage an Endpoint Detection Solution

Businesses often have dozens or hundreds of remote endpoints, such as computers and servers. These endpoints are difficult to continuously monitor with traditional anti-virus software and are a favorite vulnerability point for cyber attackers. An **endpoint detection solution** uses artificial intelligence (AI) techniques to identify suspicious activity and respond immediately.

☐ Deploy an Intrusion Detection and Response (IDR) Solution

An attacker could be lurking on your business network at this very moment. According to research from the Ponemon Institute, it takes an organization almost 200 days on average to detect a security breach. Use **an IDR solution** to detect attacks in real-time and respond before losses.

TEAM POLICIES & TRAINING 04



☐ Create an Employee Education Strategy

According to the 2018 Verizon Data Breach Investigation Report, 93% of data breaches start with phishing attacks or social engineering. With the right training, you can reduce the risk of malware, stolen accounts, leaked information, unauthorized funds transfers, and more. Consider **using simulation tools that test employees** regularly.

☐ Create & Document Secure IT Policies

Be sure to have and promote IT policies that provide guidelines and rules for computer and Internet usage, BYOD, Remote Access, Privacy, and Encryption.

☐ Enforce Technology Policies

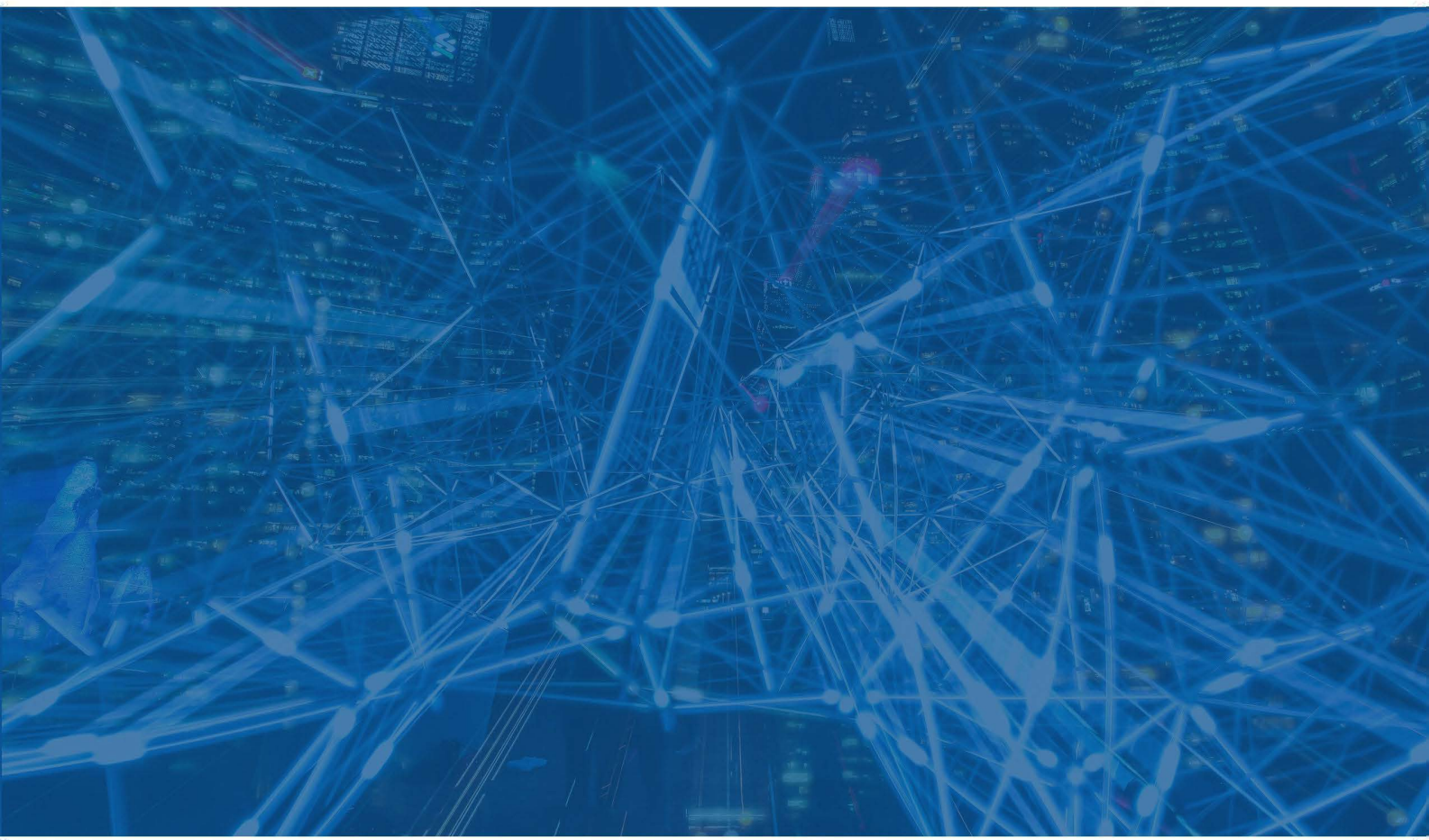
Educate team members on safe technology and data hygiene responsibilities. Whenever possible, enforce these policies through automation, such as requiring strong passwords and required password updates.

☐ Connect to Data Securely

Train staff on how to connect securely to company data when not in the office, via VPN or other secure connection. Despite security risks, a recent CompTIA study found that 94% of respondents routinely log into public Wi-Fi, and 69% of this group access work-related data over public Wi-Fi.

Keep in mind no one list can incorporate the evolving expertise and unique layered approaches that the average business requires. Ntiva clients leverage affordable solutions that together create a comprehensive cybersecurity program to safeguard your data, help meet your compliance requirements, and give you a significant competitive advantage.

If you're feeling overwhelmed or would like an expert opinion on increasing your security measure, reserve your **complimentary IT health check-up here.**



Ntiva
Managed IT, Security, & Cloud Services

7900 Westpark Drive, Suite A100 | McLean, VA 22102
1-888-996-8482 | www.ntiva.com