AVERTIUM®

eBook

2022 RANSOMWARE TRENDS

Cybersecurity events from 2019 to 2021 have given rise to ransomware and it is predicted that it will continue to rise in 2022 in a big way.

www.avertium.com

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity events from 2019 to 2021 have given rise to ransomware and it is predicted that it will continue to rise in 2022 in a big way. Attacks have become more common among the private sector, national and local government entities, and critical infrastructure organizations in recent years.

Here's what we know...

Eastern European groups don't attack each other.

They typically don't launch attacks inside the former Soviet Bloc Countries. By not enforcing international law, Russia is in effect providing safe haven to ransomware gangs, and affiliated botnet operators.

1

Check-the-box security isn't going to cut it.

When a company employs just good enough security, you can see the results in your favorite news program or blog.

2

The pandemic forced digital transformation within organizations. And that digital transformation has created an opening for attackers.

Cyber risks to businesses grew significantly as the world shifted in a more digital path in 2020 and continuing into 2022 as a result of the pandemic. Depending on which report you read, there was a substantial year-over-year spike in ransomware attacks in Q3 of 2021 compared to Q3 of 2020 and 2019.

3

While some industries are targeted more than others, anyone could be breached.

While industries (Financial, M&A, Strategic Planning, etc.) that handle large amounts of personally identifiable information (PII) are disproportionately impacted, ransomware-as-a-service operators - and in some cases, their Botnet partners - do not discriminate. But the question still remains, **who do these threat actors target?**

4

ATTRACTIVE INDUSTRY TARGETS

Healthcare

Healthcare institutions hold a ton of personally identifiable information, making them **prime targets for ransomware attacks**. With SSN, CCN, Home Address, Phone # - basically everything needed for identity theft - the fact that healthcare organizations are behind from a cybersecurity standpoint is troubling. That, coupled with many users and a mandate to protect patients - attackers know that they're easy to breach and eager to pay.

Miltenyi Biotec Case:

At Miltenyi Biotec, around 2,500 workers from 28 countries work on developing cell research and therapy products for physicians and researchers working on Covid-19 vaccines. To their surprise, a ransomware attack hit this multinational biomedical and clinical research business, affecting the company's global IT infrastructure. The company stated that the malware source will be disclosed. However, because Miltenyi Biotec quickly detected and contained the attack, the company successfully restored all impacted operating processes, though some ancillary services in some countries were still experiencing issues. Given the global pandemic, this one could've been extremely detrimental.

Miltenyi Biotec - North America

Fintech

According to Fintech News, **Covid-19 is blamed for a 238% increase in cyberattacks in FinTech**, with **80% of firms investing in digital infrastructure enhancements worldwide.**

After detecting a ransomware attack, Finastra, a financial technology firm that provides technology solutions to banks, was forced to shut down their key systems globally. That said, really anyone - even a world famous sports team - can fall victim.

Manchester United Football Club

Manchester United Football Club:

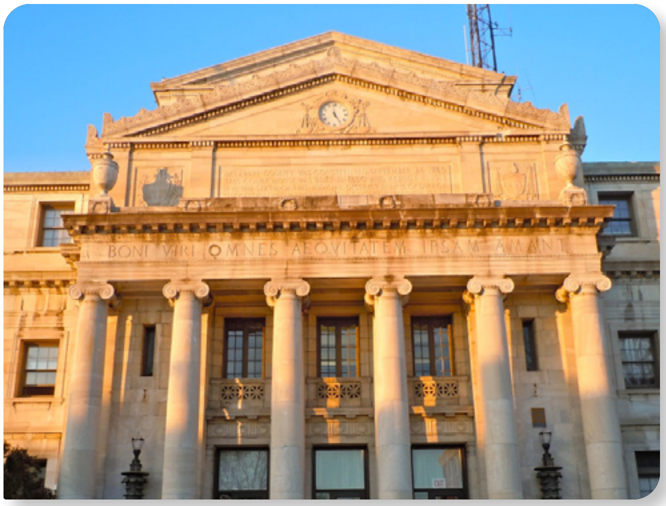
Manchester United is a top professional football club based in England that competes in the Premier League. Like many attacks, a [vulnerability was found](#) in one of the club's technologies (assumed to be a computer). After spotting the virus, Manchester United quickly shut down all systems - affected and unaffected - to contain the damage and protect data. The club later revealed that, despite the sophisticated nature of the ransomware attack, they had up-to-date, detailed policies and procedures in place that prepared them for such an incident.

Governments

Ransomware is a powerful weapon against governments. In particular, those who provide a public service and can't afford the greater cost of data restoration, lost revenue, and reputational damage. As a result, paying the ransom is seen as the logical solution.

Delaware County of Pennsylvania:

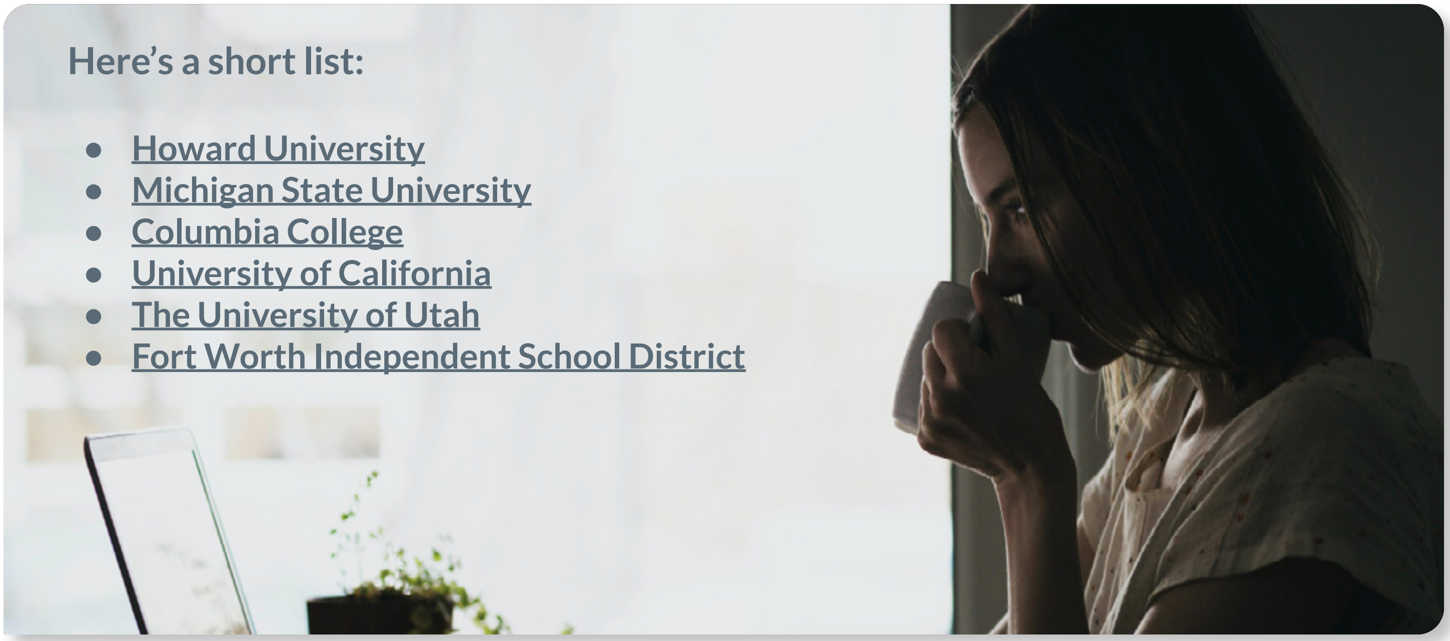
The County of Delaware was unaware of a ransomware attack until members discovered a disruption in several of the county's computer networks. Immediately after, the county partnered with computer forensic experts to assess the extent and severity of the incident, and systems were taken offline. Further investigations concluded that the attack was led by the ransomware gang, DoppelPaymer. Although emergency services were unaffected, the county chose to pay the [ransom of $500,000](#) and worked diligently to restore all system functionality.



Delaware County, PA

Education

With a number of educational institutions hit during 2020 and 2021, many **more will be hit in 2022**. Educational institutions tend to have limited budgets to begin with and pour most of that into student education. As a result, limited budgets, outdated systems, and competing priorities prevent cyber hygiene from being a top priority.



Here’s a short list:

- Howard University
- Michigan State University
- Columbia College
- University of California
- The University of Utah
- Fort Worth Independent School District

SIX TRENDING RANSOMWARE THREATS

Infected Manufacturing Processes - Insider Threats

The attack on supply chains causes distrust in technology we rely on. **Every year,** **more than 34%** **of businesses globally are affected by insider threats.** Forrester researchers believe the remote-workforce trend will drive an uptick in insider threats.

Insider Threat Average
34% +
0%
100%

BREACHES TIED TO INSIDER THREATS ANNUALLY

Third Party Risk

Ransomware attacks on third party vendors are not new. However, the increasing attacks reveal that ransomware threats towards third parties are becoming more prevalent. Even if your organization follows best cybersecurity practices, ransomware gangs can still find a way to infiltrate - simply, by looking for vulnerabilities within your third parties.

Serving as a "soft target", attackers choose third party suppliers and partners instead of attacking head on. This is typically due to third parties having weaker defenses than the larger organizations with enterprise-level cybersecurity. As a result, data exfiltration becomes an easier process for threat actors, which is why it's important for organizations to look beyond their environment when assessing ransomware risk. **Continuous monitoring is a proactive approach** to identify, prioritize, and remediate against vulnerabilities, and in return, effectively closing an attacker's window of opportunity.

Phishing + Spear Phishing Attacks

Phishing and spear phishing are common forms of delivering ransomware payloads. Both are designed to grab your attention and have you perform a specific action - typically clicking on a malicious link. But what's the difference? Well, in short, the difference is dependent on the attack target.

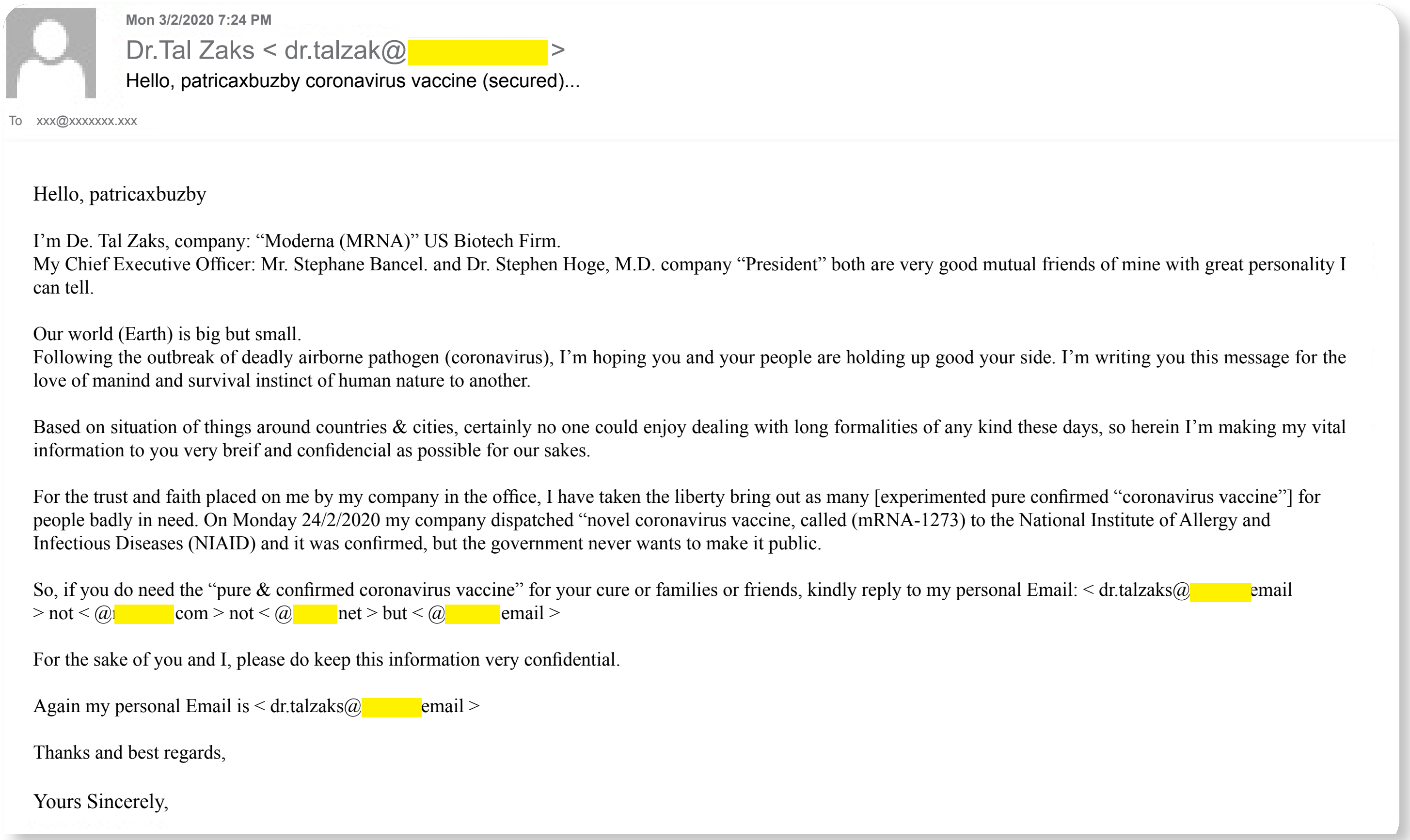
Phishing emails are sent to a **mass network** of members at a specific organization with the expectation of finding at least one vulnerability, or respondent. As for spear phishing, these emails are carefully **curated to target a single recipient**, usually for one specific purpose. With automation and machine learning getting better and better, researchers warn that enterprises should expect a "major increase" in spear phishing attacks in 2021 well into 2022 as automation enables personalization at a large scale. The information gathered from the respondent(s) could then be used for identity theft, obtaining company login credentials, and more. A few notable email techniques can be seen as job offers, impersonation of common applications, and even morse code.

22% OF BREACHES INVOLVED PHISHING

45% OF BREACHES FEATURED HACKING

17% OF BREACHES INVOLVED MALWARE

Verizon



Mon 3/2/2020 7:24 PM

Dr.Tal Zaks < dr.talzak@[redacted] >

Hello, patricaxbuzby coronavirus vaccine (secured)...

To xxx@xxxxxxx.xxx

Hello, patricaxbuzby

I'm De. Tal Zaks, company: "Moderna (MRNA)" US Biotech Firm.
My Chief Executive Officer: Mr. Stephane Bancel. and Dr. Stephen Hoge, M.D. company "President" both are very good mutual friends of mine with great personality I can tell.

Our world (Earth) is big but small.
Following the outbreak of deadly airborne pathogen (coronavirus), I'm hoping you and your people are holding up good your side. I'm writing you this message for the love of manind and survival instinct of human nature to another.

Based on situation of things around countries & cities, certainly no one could enjoy dealing with long formalities of any kind these days, so herein I'm making my vital information to you very breif and confidencial as possible for our sakes.

For the trust and faith placed on me by my company in the office, I have taken the liberty bring out as many [experimented pure confirmed "coronavirus vaccine"] for people badly in need. On Monday 24/2/2020 my company dispatched "novel coronavirus vaccine, called (mRNA-1273) to the National Institute of Allergy and Infectious Diseases (NIAID) and it was confirmed, but the government never wants to make it public.

So, if you do need the "pure & confirmed coronavirus vaccine" for your cure or families or friends, kindly reply to my personal Email: < dr.talzaks@[redacted]email > not < @[redacted]com > not < @[redacted]net > but < @[redacted]email >

For the sake of you and I, please do keep this information very confidential.

Again my personal Email is < dr.talzaks@[redacted]email >

Thanks and best regards,

Yours Sincerely,

Example of a phishing email

With both forms being a huge threat, organizations can take steps in putting both technical and human controls into place to limit the threat damage. Along with standard practices such as spam filters and antivirus, organizations can conduct phishing simulation tests, as well as establish processes on how to spot and report suspicious emails to the security team.

Attacks on Critical Infrastructure

Whether it's hydroelectric power generators or nuclear power plants, critical infrastructures create an "energy grid" that provides for the people.

So, as the infrastructures become more complex and reliant on connected technologies, it opens the network up to far more vulnerabilities. And because of this interconnectivity, the failure of one sector or critical infrastructure could **result in a catastrophic chain reaction**. From the 2019 ransomware attack on aluminum production at Hydro, to the 2021 ransomware attack on the gasoline supplier, Colonial Pipeline, cyber attacks on critical infrastructures are becoming more prevalent, more sophisticated, and more disruptive.

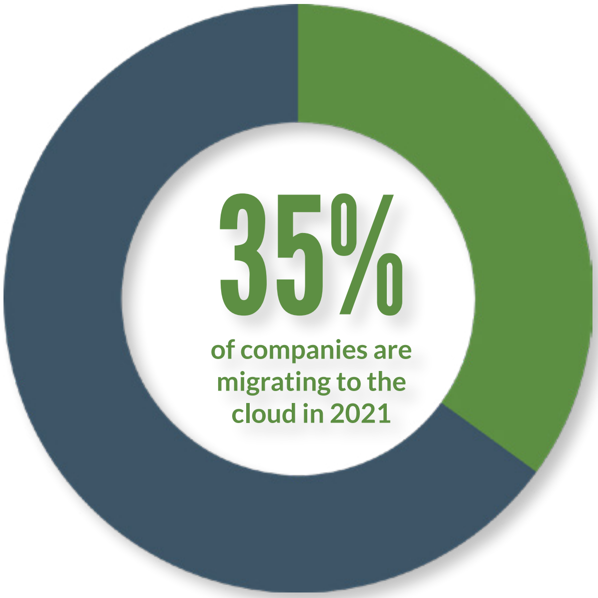
The key to building trust in your systems begins with having zero trust across your entire network. Also note that it's just as important to have an incident response plan to prepare for and to mitigate incidents.

Multi-Cloud Environments Expand Your Attack Surface

Forrester Research claimed that, *"Cloud took center stage in the pandemic recovery."*

Encouraged by work-from-home realities, cloud adoption continues to accelerate with the help of software-as-a-service (SaaS), cloud-hosted processes and storages. The proliferation of available cloud services used by organizations often result in increased complexity and increased vulnerability within the organization's security walls. With a disparate collection of cloud technologies in place, it's harder to keep up with each one's security controls. Leading to an inexorable truth: **When your environment expands, your attack surface expands with it**.

A study by Rebyc found that **35% of companies** surveyed said they plan to **accelerate workload migration to the cloud in 2021**. With no signs of slowing growth, by the end of 2022 the migration to multi-cloud environment is expected to rise even higher.



Each time a new cloud environment is added into the system, whether as infrastructure-as-a-service from the big three – AWS, Google Cloud, Microsoft Azure – or software-as-a-service that you're transmitting data to or from, there is an increased risk that needs to be managed. To gain full visibility of all possible attack surfaces, organizations must monitor and ensure smooth controls across all cloud infrastructures.

IoT Devices are Becoming More Vulnerable Due to 5G Technology

More than 93% of healthcare organizations experienced a data breach in the past three years, according to Herjavec Group. Some experts think that 5G wireless networks could signal a possible fourth industrial revolution. Expected to be 500 times faster than our current wireless network, 5G dramatically reduces the time it takes for a technology to receive and process its command before execution.

With faster connection, your devices have the ability to instantly connect with one another, making your network even more vulnerable. In short, **instant connection = instant acess to all of your data points**.

STEPS YOU CAN TAKE TO PROTECT YOUR DATA

Protecting your data starts with approaching your cybersecurity maturity from a holistic perspective - which means looking at the **people**, **processes**, and **technologies** underpinning it.

Addressing the Human Element

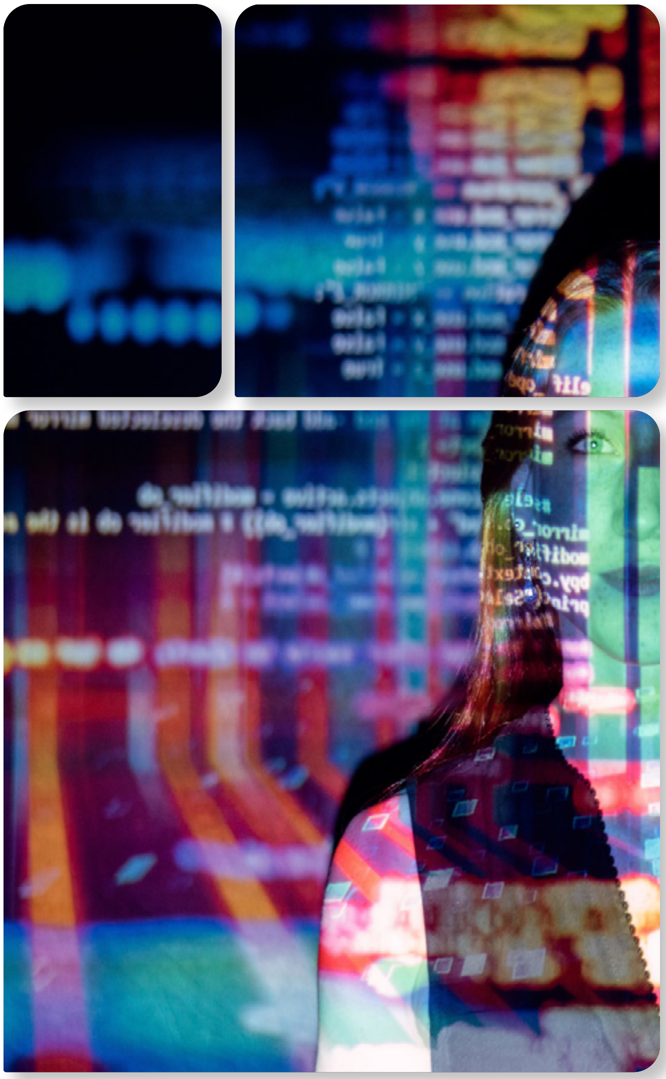
Employee Awareness:

Not everything dealing with reducing risk is technology-related. As an end user, the best way to avoid being exposed to ransomware - or any type of malware - is to be a cautious and conscientious computer user. Ransomware Gangs have gotten increasingly savvy, so you need to be careful about what you download and click on. It's best to hover over a link before you click to see where it might take you. If it looks suspicious, pick up the phone and call the originator first.

Certainly, you want to implement technology and controls to reduce certain attack vectors - known and unknown alike. You can also educate employees on cybersecurity awareness, addressing things like:

- How to spot a suspicious link
- How to securely work from home or remote work environments
- How to gauge the safety of a particular website

Educating employees on basic cybersecurity hygiene just might make the difference the next time an attacker targets your organization.



Password Protection:

Use strong, complex passwords. Regularly change them - never reuse. And consider utilizing a password vault.

3rd Party Vendors:

Ask them questions!

- How are you protecting my information?
- What are you doing with my information?
- Where are they physically located?
- What is your procedure for notifying me of an incident?
- Are you encrypting all our data at rest, and if so, with what method or algorithm?
- What infrastructure is your third-party vendor using?

Addressing the Process Element

Invest in Network Segmentation:

By dividing your network into smaller segments, you limit the lateral spread of ransomware / malware. Patient Zero may be infected, but the rest of the network can be spared as the malware looks to expand. With network segmentation, you can also configure your firewall in order to restrict or fully block remote desktop protocol (RDP), as well as, other remote management services at the network level. For instance, to avoid compromised emails from reaching users' inboxes, use spam-detection methods such as spam lists or restrict file extensions from being sent via email.

Conduct Periodic Penetration Tests:

Penetration testing, also commonly referred to as "adversarial security testing" or "offensive security", enlists ethical hackers to put your cybersecurity strategy to the test. Through the simulation of real-life tactics, techniques, and procedures employed by bad actors, pen tests can reveal blind spots in your security posture, offer context around potential threats, and enable your organization to plan and prioritize your cybersecurity investments accordingly.

Ensure You're Up-to-Date on the Latest Security Patches:

Patching operating systems, software, and firmware as soon as manufacturers release updates is vital.

Always Have Data Backup and Retrieval at the Ready:

Make daily backups of your critical data and store them offline (preferably offsite) so they can't be accessed via your network. By storing your data offline, you're creating another layer of defense. It's also critical to test the data backup process on a regular basis to ensure that backups are capturing all critical data and that the restoration process works in your environment. And check that the files can be accessed from the backup on a regular basis. You don't want to find out you can't recover data from backups when you need it most.

Design an Incident Response Plan:

If the worst case scenario does come to fruition, it's important to have everything you need to spring into action. An effective incident response plan balances business continuity, evidence retention, containment, and recovery.

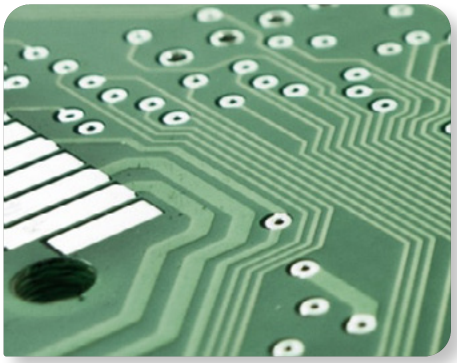
Consider a Zero Trust Network Access (ZTNA) Approach:

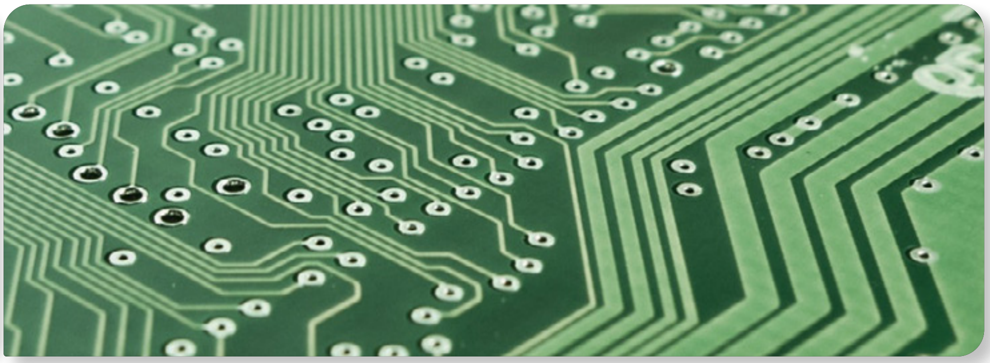
With the vanishing network perimeter, expanding endpoints, and hybrid cloud environments, ZTNA offers a way to enhance visibility and control access.

Leverage NIST CSF to Ensure that You're Covering All of Your Bases:

With most organizations lacking a unified cybersecurity strategy, the NIST CSF framework offers both clarity and structure for organizations looking to understand where they stand on the continuum of cybersecurity maturity.

Addressing the Technology Elements





Reduce Attack Surface:

Block inbound RDP from the Internet and rapidly patch your infrastructure when vulnerabilities are disclosed - especially your firewalls and VPN infrastructure, as these are the most common entry points for ransom operators.

Test Phishing Attacks:

Deploy simulated phishing attacks (widely available as free online services) that test unsuspecting employees and generate reports on who opens malicious emails, how fast, and what it can mean for your organization if the attack was real.

Strengthen Security + Access Controls:

Enable two-step authentication, deploy CAC, Smart Card, or biometric authentication in addition to secure passwords.

SIEM:

Organizations will never be able to completely stop the threat of ransomware attacks. So, they must have appropriate threat detection and response capabilities to be able to reduce time to detection and automatically orchestrate a response to remediate the threat.

Extended Detection + Response (XDR):

Just as EDR was an improvement on previous malware detection and antivirus capabilities, XDR represents an evolutionary advancement designed to deliver enhanced performance relevant to today's demanding threat environment. With broader, yet more contextualized capabilities, XDR enables companies to identify and prioritize threats, using AI and machine learning to enhance automation and analyze data more effectively.

Managed Detection + Response (MDR):

For organizations that have adequate cybersecurity monitoring in-house (or through an MSSP) but want or need to upgrade their incident detection and response capabilities, an MDR is probably the right choice. These service providers are focused on finding and remediating potential threats on your network to minimize your probability of regulatory non-compliance.

HOW AVERTIUM CAN HELP YOU DETECT & MITIGATE RANSOMWARE

Being susceptible to ransomware threats is something that organizations can't stop, but with the proper controls in place, you can minimize and manage the attack surface to stop most attacks before they start. There are no guarantees that every attack will be stopped, so it's important to have a remediation plan in place for that worst case scenario.

However, if you become a ransomware victim, focus on mitigation prevention and containment:

- **Extended Detection & Response:** We believe that XDR in all of its forms - tools, platforms, services - is fundamentally an approach, not a toolset. Rather than point solutions that claim to be "XDR," Avertium employs XDR as a philosophy, delivering on the promise that XDR makes: the right combination of innovative technology, field-validated threat intelligence, and resource empowerment to reduce complexity, streamline your operations and expertly manage your attack surface.
- **Zero Trust Network Architecture:** As a key component of Avertium's rigorous approach to providing extended detection and response (XDR), ZTNA gives our customers more visibility into data across networks, the cloud, endpoints, and applications.
- **Digital Forensics and Incident Response:** Provided as an on-demand crisis response service as well as retainer-based program, Avertium's Digital Forensics and Incident Response (DFIR) helps you to rapidly assess, contain, eradicate, and recover from a security incident to minimize impact and return you to normal operations.

Ransomware gangs understand the current challenges faced by organizations in a work-from-anywhere environment and a collapsed perimeter - they view this as a segue into extorting data. The time it takes to detect, contain, and respond are very challenging in an unprepared company.

Having a higher level of visibility shines a spotlight on unauthorized users faster, allowing for enhanced containment and stronger, more timely incident response. Avertium's team of industry experts can help you implement cutting-edge monitoring and detection technology (EDR) to meet the challenges of today, and prevent the threats of tomorrow.

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium** when they want to be more efficient, more effective, and more resilient when waging today's cyber war. Show no weakness.®

1

Business Continuity without Compromise

Our business-first philosophy positions security as a path to innovation instead of a blocker. From the alert to the boardroom, Avertium arms you with everything needed to make informed decisions that balance safer paths to business continuity today, and measurable security maturation tomorrow.

2

Human-Centered Approach

Avertium brings humanity back into the realm of cybersecurity, giving you better security strategy from highly experienced professionals who can act faster because they know you, know your systems, know your business, and know what they're doing. We approach security as a continuum and not as a point in time; we bring context to the chaos, giving you everything you need and nothing you don't.

3

XDR as a Philosophy

With our XDR philosophy at work, we build a customized security program tuned to your unique environment and risk profile. In doing so, we deliver the right technology - not all of the technology - which enables you to see every threat, extend your reach, adapt, and attack.

CONNECT WITH US

AVERTIUM®

CyberOps Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

This publication contains general information only and Avertium is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Avertium shall not be responsible for any loss sustained by any person who relies on this publication.

| Privacy Policy

#SHOWNOWEAKNESS™