ARCHERPOINT

Cybersecurity Threats & Countermeasures

PROTECTING YOUR COMPANY FROM EXTERNAL AND INTERNAL THREATS

Contents

Introduction

TODAY'S COMPANIES ARE FACING CYBERTHREATS DAILY.

A single security breach could cost a company hundreds of hours in lost work hours repairing the damage, loss of intellectual property, and millions of dollars in lost revenue due to theft, ransomware, and regulatory fines and penalties.

Even as new preventative measures are developed, cybercriminals are finding new ways to circumvent them. The threats are real and are not going away.

Our team of application and data security experts have put together this eBook to help our clients stay current on cybersecurity threats and countermeasures. ***In this volume, we cover:***

- Steps toward protecting your cloud applications from bad actors.
- A framework for responding to a ransomware attack.
- Preventing your company and your employees from falling victim to phishing attacks.
- Using open-source intelligence (OSINT) to protect your company from external threats.
- The importance of strong password protection and multi-factor authentication – now more than ever.
- And protecting your business from internal threats and occupational fraud.

Start securing your company now with ArcherPoint's ***Cybersecurity Threats and Countermeasures: Protecting your company from external and internal cyberthreats.***

DID YOU KNOW

In 2022, there was nearly 200 million ransomware attacks in the US, according to the **2023 SonicWall Cyber Threat Report**.

Protecting Your Cloud Applications from Unauthorized Access

ALL COMPANIES MUST TAKE STEPS TO PREVENT UNAUTHORIZED ACCESS TO THEIR CLOUD APPLICATIONS. HERE ARE SOME BEST PRACTICES TO FOLLOW.

Most businesses are running at least one of their critical business applications in the cloud, such as their ERP, CRM, or Payroll, to take advantage of many of the efficiencies of cloud apps: lower maintenance costs, automatic updates, and anytime/anywhere access.

While all the major application hosting providers offer robust security features, it is still important for companies to take steps to maintain privacy, secure sensitive data (including intellectual property and customer data), and prevent unauthorized access. ***Here are some best practices for securing your cloud applications:***

1

USE STRONG AUTHENTICATION

To enhance security and prevent unauthorized access, it is recommended to implement robust authentication mechanisms like multi-factor authentication (MFA). This method adds an extra layer of protection by requiring users to provide additional verification factors, such as a code sent to their mobile device or email address.

2

EMPLOY DATA ENCRYPTION

Use secure communication protocols (e.g., SSL/TLS) to protect data transferred between users and the cloud application. In addition, use encryption to safeguard sensitive data stored in databases or file storage systems.

3

STAY CURRENT ON SOFTWARE UPDATES AND PATCHES

Software updates often include security patches for known vulnerabilities. Make sure that these updates are installed quickly. Also, be sure to maintain other components of your cloud application, including the operating system, web server, and database.

4

IMPLEMENT STRONG ACCESS CONTROLS

Most applications allow administrators to grant or deny read/write access to specific user types or roles. Be sure to limit user permissions and restrict access to sensitive data and functionality. Follow the principle of least privilege, granting users only the privileges necessary for their specific roles.

5

IMPLEMENT REGULAR LOGGING AND MONITORING

Enable logging mechanisms to record and monitor activities within your cloud application. Set up intrusion detection systems to identify and mitigate potential threats. Regularly review logs to identify any suspicious activities.

6

CONDUCT REGULAR SECURITY ASSESSMENTS

Perform periodic security assessments, including penetration testing and vulnerability scanning, to identify and address potential weaknesses in your cloud application to help you stay ahead of new threats and ensure ongoing security.

7

IMPLEMENT DATA BACKUP AND DISASTER RECOVERY PLANS

Regularly back up your data and develop a comprehensive disaster recovery plan to mitigate the impact of potential data breaches, system failures, ransomware attacks, or other incidents. Test your backup and recovery processes regularly to ensure their effectiveness.

8

MAINTAIN COMPLIANCE WITH INDUSTRY REGULATIONS

Certain industries and governments have rules and regulations governing the security of cloud-based applications and data. Maintaining compliance with these regulations is essential to avoid significant fines and loss of customer confidence.

9

EDUCATE YOUR STAFF

Provide security awareness training to your employees to help them understand common security risks and best practices. Ensure they know how to respond to various attacks and the proper escalation procedure once a security incident has been identified.

10

REGULARLY REVIEW AND UPDATE SECURITY POLICIES

Maintain up-to-date security policies and procedures that align with industry best practices. Periodically review and update these policies to address evolving security threats and changes in your cloud environment.

Safeguard your cloud applications

Security is an ongoing process, and it's crucial to stay updated with the latest security practices, follow vendor recommendations, and monitor security advisories to keep your cloud applications secure.

You can effectively safeguard your cloud applications from potential threats by staying proactive and up-to-date.

How to Respond to a Ransomware Attack: A Framework for Companies

RANSOMWARE ATTACKS CAN HAPPEN AT ANY TIME. HERE ARE THE STEPS TO TAKE IF YOUR COMPANY IS A VICTIM OF AN ATTACK.

Ransomware attacks can have devastating consequences for an organization. Some victims of these attacks could not retrieve all their lost data, even after paying the ransom (let's face it, attackers do not set up a support team to help you get your data back once they have your money!). Other companies have paid the ransom, only to be met with subsequent ransom demands from their attackers.

According to **SonicWall**, there were 493.3 million ransomware attacks worldwide in 2022 and more than 200 million in the US alone. Although the number of attacks is down more than 20% from 2021 (largely due to better attack prevention and response techniques), attackers respond by increasing the amounts demanded. Ransomware poses a clear and present danger to businesses, governments, healthcare providers, and educational institutions worldwide.

An ounce of prevention is worth a pound of cure

The reality is that prevention offers a better ROI than reacting to an attack. Moreover, companies should adopt the attitude of what they will do WHEN an attack occurs, not IF. Assuming that an attack is inevitable helps to ensure safeguards are prioritized and implemented quickly.

All companies should have security plans to protect themselves from ransomware attacks. Maintaining security updates to your devices and networks, enforcing cyber-hygiene practices across the organization, and regularly performing and testing backups are actions that can minimize the impact of an attack when it does occur.

Keeping devices up to date is critical to securing you from attacks. For example, the recent Log4j attacks exploited vulnerabilities that had already been identified and fixed, but the fix had not been installed.

Firewalls can only help so much. A number of out-of-date servers and devices contributed to the severity of the attacks. That said, only a small percentage of ransomware attacks leverage system and network vulnerabilities.

More often than not, cybercriminals gain entry through the unsuspecting actions of users who fall prey to phishing emails and various social engineering tactics.

User education needs to be your top priority for ransomware prevention. Training your employees with the knowledge and skills to recognize and report phishing emails is crucial, as these remain the primary avenues for ransomware delivery.

What to do in the event of a ransomware attack

If your organization does fall prey to a ransomware attack, it is crucial to respond quickly to minimize the impact. ***Below are some recommended actions to take in the event of an attack:***

1. ISOLATE AND DISCONNECT

Isolate and disconnect any affected system from the rest of the network to prevent spread.

2. ASSESS THE IMPACT

Determine the scope of the attack and identify the systems, files, data, intellectual property, and any other company assets that might have been affected.

3. REPORT THE ATTACK

Promptly notify internal stakeholders, such as IT, management, and legal. Determine if you must also report to law enforcement or regulatory agencies.

4. BRING IN EXPERTS

Involve cybersecurity experts specializing in ransomware attacks to help with investigation, containment, and recovery efforts.

5. PRESERVE EVIDENCE

Collect and secure intact data, such as capture logs, files, and other evidence, to identify the attacker's actions.

6. COMMUNICATE WITH STAKEHOLDERS

Be transparent. Regularly ommunicate with employees, customers, suppliers, and other stakeholders about the incident and the subsequent actions being taken.

7. RESTORE FROM BACKUPS

Ransomware attackers can wait weeks before attacking. Attempt to restore the systems targeted with uncompromised backups that date prior to when the attack appeared on your system.

8. CONSIDER YOUR OPTIONS

Involve your legal counsel, law enforcement, and cyber response experts if you are considering paying the ransom. Remember, it does not guarantee you will retrieve any of your data.

9. CONDUCT A REVIEW

Perform a thorough review of the incident. Identify the weaknesses in your security, then update your security measures based on the review results.

Just When You Thought It Was Safe to Go Back in the Water... Phishing, Quishing, Vishing, and Smishing

HACKERS USE SOCIAL ENGINEERING TO GAIN ACCESS TO PERSONAL INFORMATION, INTELLECTUAL PROPERTY, AND GOVERNMENT SECRETS. LEARN THEIR TRICKS AND HOW TO FIGHT BACK.

The term "phishing" describes emails sent by malicious hackers to coax the email recipient (the victim) into clicking on a link that asks them to divulge personal information or login credentials. Sometimes, the victim's computer is infected with malware that could damage files, steal data from the device, or intercept secure communications (such as with their bank, credit card company, or investment firm).

What are the common elements of phishing?

Phishing is a form of social engineering designed to make the target take an action without giving it much thought. The malicious email contains "bait" that the attacker hopes the victim will click on. ***Typical phishing attacks use variations on several themes:***

An email from a familiar brand advising that their account has been compromised.

An email that threatens legal or financial penalties if an action is not taken.

An email with the promise of a valuable prize. "Register to win - you MUST act now!"

Phishing variations

Many companies have instituted email screening programs to protect employees by identifying and removing suspicious phishing emails. Of course, that only leads to bad actors finding alternative methods to get what they want. So now, in addition to phishing we have ***quishing***, ***vishing***, and ***smishing!***

"Quishing" is a form of phishing attack where an email is sent to the target with the same threats or enticements and sense of urgency as a phishing email but use a Quick Response (QR) code to send the victim to the hacker's URL.

Since the malicious link is an image (a QR code) rather than a text string (URL), it becomes harder for email filters to identify a possible attack. Once the victim takes the link in the QR code, they are "hooked."

"Vishing" has the same tactics as phishing but uses voice via telephone calls to socially engineer the victim into divulging their personal information – account numbers, social security numbers, birth dates, etc. Vishing attacks might use a live person, a computer-generated voice, or a combination.

In another variant, "smishing" uses SMS (mobile phone text messages) to fool victims into taking a link and surrendering their information. Common smishing attacks pretend to be bosses, CEOs, and managers who call with a sense of urgency where "something has gone wrong" and they need your login info immediately.

Protecting yourself

In all these attacks, the common theme is to get the victim to take a link or divulge personal information, usually using a scare tactic. ***The best way to protect yourself is to remain vigilant:***

- **BE AWARE OF SOCIAL ENGINEERING TACTICS**
  Savvy hackers research their victims, scanning social media profiles, looking for anything to give their communication a sense of legitimacy.

- **VERIFY THE LINKS ARE GENUINE**
  If an email looks suspicious, verify the sender's address and any links within the body of the email.

- **LOOK FOR MISSPELLINGS AND ODD PHRASING**
  Legitimate businesses proofread their communications. They will not send out a poorly worded message with multiple misspellings.

- **BE ON THE LOOKOUT FOR A FALSE SENSE OF URGENCY**
  Phishing works best if they can get you to act first and think later. This is true in business as well as personal life.

- **BEWARE OF ATTACHMENTS**
  Don't open files you are not expecting, particularly from unknown senders. If you're unsure, call the individual first to see if they sent you the file.

- **BE CAREFUL USING PUBLIC WIFI**
  Public WiFi typically provide unsecured access. It is better to use your phone as a personal WiFi hotspot or set up a Virtual Private Network (VPN).

- **NEVER GIVE YOUR LOGIN CREDNTIALS TO ANYONE**
  If somebody, even someone you trust, needs to log into a system, tell them to contact the administrator to grant them access.

- **USE 2FA WHEN AVAILABLE**
  While not perfect, two-factor authentication (2FA) can be an effective deterrent to a cyberattack.

- **WHEN IN DOUBT, CALL**
  If you are ever in doubt about the legitimacy of a message, call the company directly. Never use the contact numbers contained in the email itself.

Remaining Vigilant:
External Threat Detection With OSINT

EVERY ORGANIZATION MUST REMAIN VIGILANT FOR POTENTIAL CYBER THREATS. LEARN HOW OSINT HELPS SECURITY TEAMS STAY CURRENT ON THE LATEST TRENDS.

For all the benefits that the internet has provided to businesses, from cloud computing giving you anytime, anywhere access to robust data analysis at the click of a button, there are also increased risks of cyberattacks that take advantage of security vulnerabilities in the networks, devices, and applications used by these organizations.

What is your attack surface?

Every internet-facing entry point your organization uses, such as services and applications, email servers, and network devices, constitutes your attack surface. This attack surface extends beyond the organization itself to include devices used by remote workers. Every point of entry has the potential of having a security vulnerability that bad actors can exploit to gain access to your network. As a company's attack surface grows, there are more opportunities for bad actors to find a source of entry and cause irreparable harm, and they only need to find just one!

Identifying external threats with Open Source Intelligence (OSINT)

Every organization must remain vigilant of its attack surface to identify potential threats and mitigate them as soon as possible. However, as the phrase goes, "You don't know what you don't know," security teams must first identify what threats are present before taking steps to mitigate them.

Many organizations monitor potential threats using Open Source Intelligence (OSINT). OSINT uses publicly available information to identify, analyze, and report potential security vulnerabilities. Public information, whether free or purchased, can be obtained from any legally available source, including the internet, social media sites, public records, publications such as magazines and newspapers, blogs, forums, corporate websites, and even the dark web.

How OSINT is used to protect against threats

OSINT helps security teams stay current on the latest cybersecurity threats and trends by collecting information on vulnerabilities and tactics and acts as an early warning system.

1

THIRD-PARTY RISK AND VULNERABILITY MANAGEMENT

OSINT can gather information on security incidents and breaches and identify disclosed vulnerabilities so the security team can prioritize patching and mitigation efforts based on how severe and relevant those vulnerabilities are. Security teams use this information to make informed decisions about the organization's relationships with these third parties. Without them, the team may never know the threats even exist.

2

PROACTIVE THREAT HUNTING

OSINT is used for real-time threat detection and containment. OSINT helps you stay current with the latest phishing and social engineering playbooks, malicious domains, and email addresses.

3

DARK WEB MONITORING

Monitor underground forums for mentions of the company's brand, employee emails, usernames, credentials, accounts, and corporate entry points. This helps the security team identify who is attacking and the typical attack patterns employed, allowing them to take proactive measures to secure exposed information.

4

BRAND PROTECTION

OSINT can also be used to look for company mentions. Bad actors sometimes masquerade as company representatives, creating posts that could damage the company's brand and reputation.

5

TEST FOR POTENTIAL THREATS

Penetration testers can use OSINT data to uncover additional risks, including data leaks (inadvertent exposure of personally identifiable information), unpatched software, and open ports.

OSINT can be used for good...or evil

Because OSINT information is available to everyone, bad actors have access to it as well. That means that, whether you are monitoring it or not, they are. ***And they are using OSINT data for malicious reasons, including:***

- ### TARGETED IDENTIFICATION
  Bad actors gather information about an individual using email surveillance and social media profiling to target the person with personalized phishing and social engineering scams. The bad actor might pose as a legitimate software vendor known to be used by the target, or they might impersonate the target's boss in a text message.

- ### EXPLOIT PUBLICLY KNOWN VULNERABILITIES
  While security teams use OSINT data to discover known vulnerabilities of platforms and applications to reduce their attack surfaces, threat actors use the same information to hunt for and exploit unpatched systems.

- ### DARK WEB DATA
  Threat actors can search the dark web for mentions of the company's brand, employee emails, usernames, credentials, accounts, and corporate entry points to leverage in a targeted attack. They can even purchase previously compromised user credentials.

Password Security and Protection Has Never Been More Important

FOR YEARS, THE RULE HAS BEEN TO USE A COMPLEX PASSWORD. NOW, HACKERS CAN CRACK COMPLEX PASSWORDS IN MINUTES.

How secure is your password?

For years, the rule has been the more complex the password, the more challenging it was for a hacker to access your account. Password complexity is a function of how many characters you use and whether you include a combination of upper- and lower-case letters with numbers and symbols.

Until recently, that seemed reasonable. According to the cybersecurity company **Hive Systems**, a relatively complex password of nine characters using numbers, mixed-case letters, and symbols would take a hacker three weeks to crack using brute force...in 2020. This figure was based on the processors and software that were readily available in 2020 and could be used to crack passwords using brute force. In 2023, breaking that same 9-character password will only take six hours. That assumes the hacker uses high-end consumer graphics cards you can buy at BestBuy or Amazon.

Once they step up to server-grade hardware and AI-assisted models and bots to do the brute force work, cracking a complex 9-character password could only take one minute! The best advice is to choose a complex password of at least 12 characters and avoid using the same password for multiple accounts.

Other suggestions include:

- **Use a password manager** to avoid reusing the same password for multiple accounts.
- Use a passphrase of 4-5 random words with spaces as your password because **password length is more important than complexity**.
- **Reducing reused passwords** is the best thing you can do to protect yourself.
- **Always use Multi-Factor Authentication** (MFA) if given the option for the added protection.

DID YOU KNOW

Phishing and social engineering accounts for almost **80% of password breaches** caused by hackers.

How do bad actors get your password?

A common way bad actors attempt to gain access is to try multiple combinations (brute force), hoping they will stumble on a combination that works. A refinement of the brute force method is to try a series of commonly used passwords or phrases against a known user ID, hoping one is correct.

Yet a different tactic is to acquire a list of usernames obtained from a data breach and use a single, commonly used password against each username. As it turns out, brute force represents only a small percentage of attacks. **Phishing and social engineering** account for nearly 80% of password breaches. Once the hacker has your login credentials, they will try to use it against other websites, such as social media, banks, and credit cards, hoping you repeat your passwords across your accounts.

Making your passwords stronger with multi-factor authentication

Multi-factor authentication (MFA) is a process that uses more than one authentication method. Two-factor Authentication (2FA) is a common form of MFA that makes the login process more secure. Using 2FA, simply entering your username and password is not enough.

Once you successfully enter your credentials to log into a site, the site will send you a code through other means to verify that it is you, such as text message, biometrics (fingerprint on your phone), or email. This way, the hacker will also need access to your phone or email to complete the login process. While not foolproof, 2FA adds an extra layer of protection, making hacking much more difficult. In addition, 2FA is easy for the user to use and relatively inexpensive to implement.

Utilizing conditional access policies

Organizations should not rely on MFA alone and should set up additional methods of authentication that rely on Conditional Access policies to make access more "phish-resistant". ***For example:***

- If an employee is based in the United States and there is no reason why they should be accessing the system from outside the country, a conditional access policy can notify the administrator for authorization before granting access.
- A conditional access policy can be used to prevent logins from using the same user credentials from two different parts of the world.
- A conditional access policy can be set up to prevent logins for employees after business hours without administrator approval.

Conditional Access policies can also narrow down logins by specific location, device, IP Address, application, and individual, if necessary.

Take a Look at Yourself: Addressing Internal Threats and Occupational Fraud

NOT ALL CYBER THREATS ARE EXTERNAL. SECURITY THREATS CAN EXIST INSIDE AN ORGANIZATION AS WELL. FIND OUT HOW YOU CAN ADDRESS OCCUPATIONAL FRAUD.

Keeping your company's data safe from prying eyes is vital. You must have a clear understanding of where data is located, who can access that data, the regulations that apply to the data's security, and how the data can be recovered in the event of an attack.

It is important to realize that threats are not always external to the organization. Threats can also exist within the organization itself, including employees, vendors, and partners—even executive management. It's not enough to know who has access to your systems. You also need to know what they are doing with that access.

Occupational Fraud Facts

In their **Occupational Fraud 2022: Report to the Nations**, the Association of Certified Fraud Examiners researched more than 2,000 cases of fraud taken from 133 countries and 23 industries, representing a combined total loss of $3.6B. ***Here are some facts taken from that report:***

KNOW THE FACTS

- On average, organizations lose 5% of revenue to fraud each year, representing a global loss of more than **$5 trillion due to fraud in 2022 alone**.
- The average loss per case is more than **$1.7 million**.
- A typical fraud case costs an organization $8,300 per month, lasting 12 months on average before the fraud is detected.
- Nearly half of the fraud cases analyzed occurred due to a lack of or an override of internal controls.
- Anti-fraud controls resulted in lower fraud losses and faster fraud detection.

Maintaining Security With Least Privileged Access, Zero Trust, and More

Below are several recommended practices to help minimize the risk posed by internal threats.

- **DEFINE USER ROLES**
  Modern business applications allow administrators to define user roles. These roles assign privileges that identify the software applications a user can access and the actions that user can perform. Giving too much access to sensitive company information can lead to errors, fraud, and intellectual property theft.

- **LEAST PRIVILEGE ACCESS (LPA)**
  LPA assigns user roles with the minimum privileges they require to perform their job functions and no more to limit the impact one person can have on a system. LPA applies to everyone, including employees, suppliers, vendors, customers, partners, and even APIs and cloud services.

- **ZERO TRUST MODEL**
  Zero Trust is a network security model built on the assumption that every attempt to access a network or application represents a potential threat. All access requests are authenticated and continuously validated, whether they originate from inside or outside the organization.

- **SEGREGATION (OR SEPARATION) OF DUTIES (SOD)**
  Any time a single person can complete both sides of a transaction (for example, the ability to create a vendor and then authorize payments to that vendor), there is a potential for fraud. SoD requires that these types of transactions are divided between two or more people.

- **TEMPORARY ELEVATED (OR EMERGENCY) ACCESS PROVISIONING**
  There are times that require a person to temporarily upgrade their roles or privileges to a higher level of access than their job would typically need. Temporarily granting elevated privileges to an employee should also have an expiration date to ensure those privileges are automatically removed after a specified period.

- **PERIODIC ACCESS REVIEWS**
  Management should periodically review the access privileges of users on all company networks and applications to ensure Least Privileged Access is maintained.

- **SINGLE SIGN-ON (SSO)**
  SSO allows users to log into the system once and access multiple sites and applications without having to re-authenticate every time. Users only have to remember one set of credentials and administrators have greater control over user access to company applications. The downside is that setting up SSO can be complex and may pose a security risk if not properly monitored.

- **MONITOR FOR UNUSUAL ACTIVITY**
  Administrators should monitor for questionable or unusual activity. Conditional access policies can help prevent suspicious or fraudulent activity by imposing restrictions on how users can access the system based on time of day, geographic location, IP address, and more.

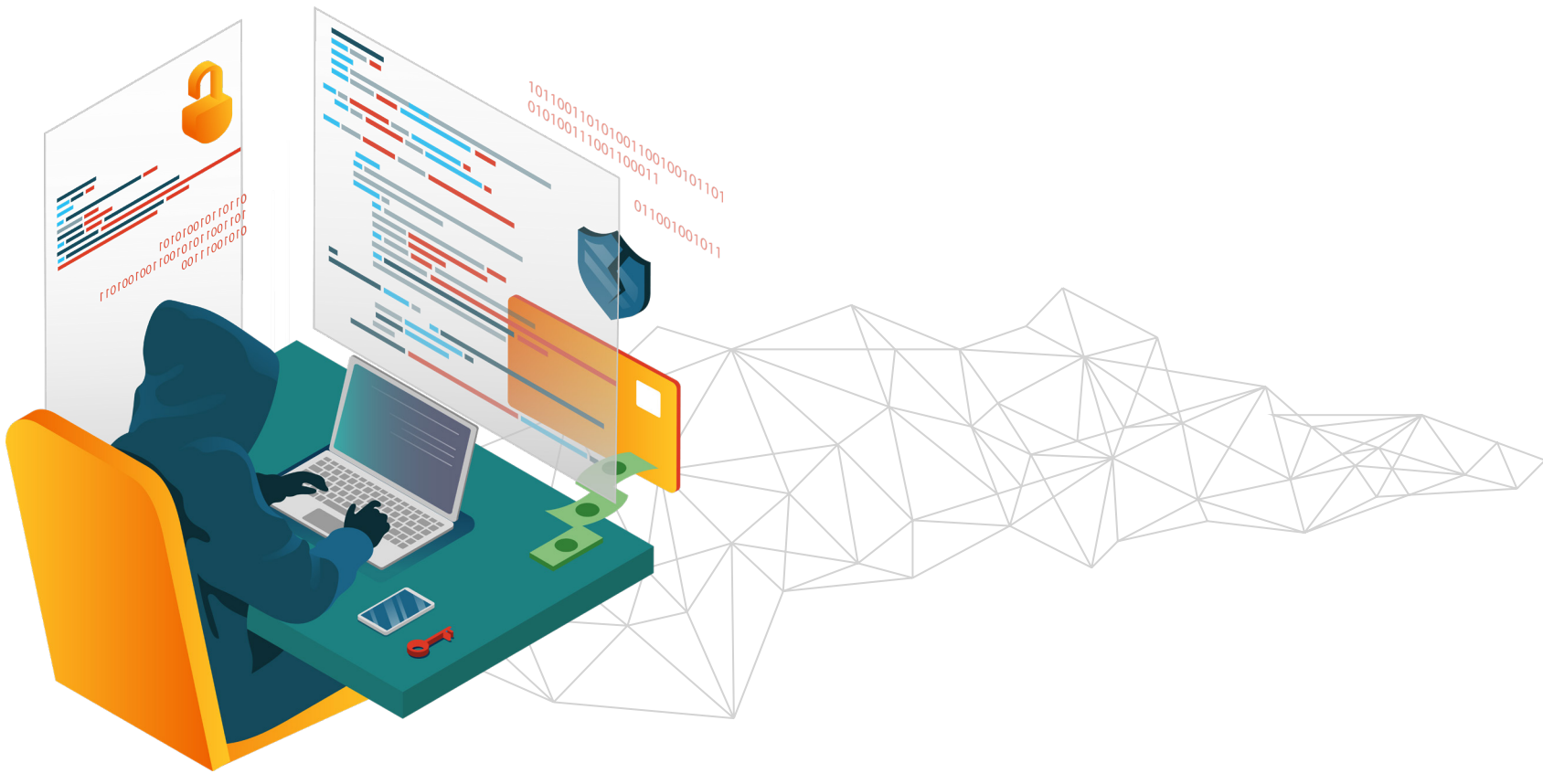
- **CONTINUOUS TRAINING ON FRAUD AND CYBERSECURITY THREATS**
  The best way to keep your company safe is to train your users, including employees, contractors, and vendors, on how to secure company networks, applications, and data. Investing in user education provides the best ROI when it comes to avoiding unnecessary risk.

Security Is an Ongoing Process

Securing your company from external and internal threats can seem overwhelming. But you don't have to go it alone. **ArcherPoint's IT Managed Services** helps companies take advantage of Azure's secure cloud environment for application and data security, risk mitigation, disaster recovery services, and more. Our network security specialists provide custom assessments, awareness training, and Azure setup and management.

Watch our webinar, **Demystifying Cybersecurity**, to learn how to start protecting your organization now and what to consider in your cybersecurity strategy, including endpoint management, password health, managed detection/response, backups, disaster recovery, and user education. ***For more information on network security and ransomware attacks, read our blogs:***

- Azure Provides Security to Prevent Ransomware Attacks
- Ransomware 'Gangs' Are Maturing, So Should Your Company Cybersecurity Policies
- Cybersecurity Business Policies Moved Forward in 2022 But Need to Improve
- Protecting Your Business Against Security Threats with Good IT Hygiene
- Clearing the Confusion Around Cloud ERP Security
- How to Address Common Security Vulnerabilities with a Zero Trust Model
- Considering Cyber Insurance? You Need a Solid Security Strategy
- Endpoint Security Management: How It Benefits Microsoft Dynamics 365 Business
- Understanding the Potential Risks of Google's New Domains



Contact ArcherPoint

ArcherPoint is dedicated to meeting all your IT needs while providing the scale and scope to adapt as cyber threats continue to evolve. Contact ArcherPoint to get in touch with an expert to learn more.

CONTACT ARCHERPOINT

Microsoft Solutions Partner