AVALONCyber

7 Ways Employees Put Corporate Data at Risk

85% of data breaches are caused by human error.

To err is human, right? While making mistakes is understandable and unavoidable, trying to avoid blunders and accidents is something every employee should strive for, especially when it comes to working online. Anticipating, detecting, and responding to cyber incidents is critical to your company's survival. But insiders – your hardworking, dedicated team members – remain the biggest threat to your corporate data.

According to a study put out by Stanford University and Tessian, 85% of data breaches are caused by human error. The report also indicates that 43% of employees are quite certain they've made mistakes that impacted security, and that one in four workers has clicked on a phishing link. These errors – whether performed unintentionally, or worse, intentionally – can cost an organization thousands, even millions, of dollars. And while large corporations that suffer a cyber incident can typically recover, at least financially, from a breach, it's much more challenging for small to mid-size companies to afford the reputational and monetary damage a breach can deliver. Which is why it's crucial to be proactive about your cybersecurity program.

But where do you even start?

First, let's look at seven surefire employee behaviors that will put your company's data at risk. Within each behavior we'll provide some tactics to implement to help improve cyber hygiene at your company. Then, we'll look at several ways in which Avalon Cyber can assist you through a range of proactive services – from policymaking to employee training – that will strengthen your organization's network.

1. Weak or Shared Passwords

It's a fact that weak passwords lead to breaches, as an adversary can brute force (meaning, they guess with or without the help of some online tools) a password in mere seconds. (Just check out the graphic on the next page from Hive Systems.)

That's why Avalon Cyber suggests all passwords be at least 15 characters with a mix of letters, numbers, and symbols, and a password is never used for more than one platform. Utilize a password manager (i.e., LastPass, DashLane, etc.) secured with a master password and multifactor authentication (MFA) to ensure that your employees create strong passwords, but don't have to remember them, as the software automatically enters and stores passwords for

them. A "sharing" issue discussed in Proofpoint's 2020 User Risk Report was that 50% of survey respondents admitted to allowing friends and family – including children – to use their work-issued device to check emails, read the news, and other "harmless" activities. Not so harmless when Little Timmy clicks on a malicious link and lets the bad guys in.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

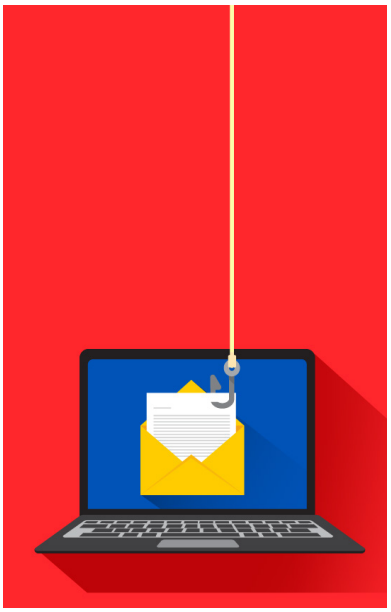
HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Source: Hive Systems

2. Bring Your Own Device (BYOD) Security Risks

A misplaced laptop. A smartphone left in the airport security line. A run for a refill of coffee while your table – and tablet – sit unattended. If these personal devices are being used by employees for work and "go missing," the corporate network and data those devices are connected to are at risk because now, everything on them is readily available to the new "owner." Many companies that implement bring your own device (BYOD) policies don't realize they're also introducing



The basic structure of phishing attacks remains the same – the user clicks, malware drops, a foothold is gained.

severe security risks. For example, they may not deploy proper security policies such as requiring users to set strict privacy settings on their devices or allowing the company to remotely destroy data if a device is lost or stolen. Another way employees put corporate data at risk is by using home computers to access corporate data – without signing into a virtual private network (VPN) first.

3. Phishing Emails

Phishing scams continue to be a problem for many companies. Despite awareness of how dangerous a phishing scam can be and repeated reminders of steps to take to make sure attachments and links are legitimate, employees continue to spread malware throughout company networks. The basic structure of phishing attacks remains the same – the user clicks, malware drops, a foothold is gained. (There are still cases where the phishing email leads users to phony sites, which are used to capture user input, but most phishing cases are used to install persistent malware.) The victim opens the email, sees the attachment that contains, for example, an invoice or resumé, and then opens the attachment. What happens next is dictated by the end goal of the phisher. The result can be ransomware that encrypts and locks all your corporate data. Or malware installed on a victim's computer that "watches" for legitimate connections to secure websites where username and password credentials are required, then scrapes those credentials, passing them back to the adversary. The bad actor can now log into secure web-based services, such as your cloud payroll provider, cloud-based hosted data, 401K accounts, and much more. One way to prevent this is to defend against email-borne threats before a human can interact with them. Email filtering at the perimeter is the first line of defense and is a no-brainer for every company. In addition, security training and testing is an absolute must, so employees learn how to recognize the latest phishing scams and techniques.

4. Unrestricted Administrative Rights

Like weak or shared passwords, users with Windows administrative credentials are very common in small to mid-size companies and pose a significant risk to corporate data. Executives and other management team members are common offenders because they frequently have access to everything. Other personnel are often granted unnecessary permissions as well. When several users have a high level of access

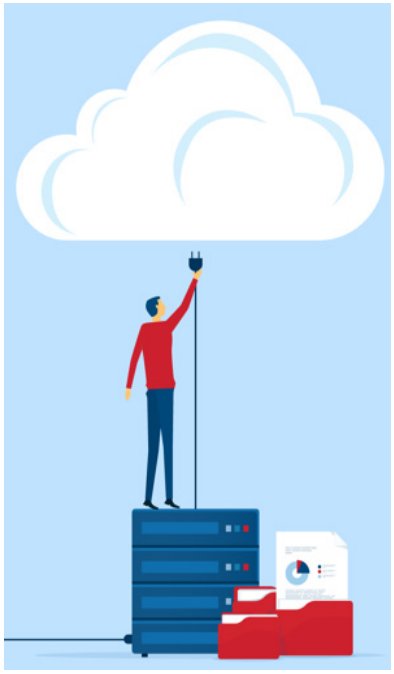
and just one of these accounts is compromised, the bad actor now has administrative privileges across the entire environment. To avoid this situation, audits of all users' rights, roles, and permissions should be conducted regularly to ensure that each user has the proper access control, and that no user has elevated or escalated their defined access.

5. Unpatched Systems and Software

Any IT professional will tell you that outdated security patches are a serious security problem. Patches are issued to fix specific vulnerabilities and security issues in an operating system or software application. Bad actors will exploit every vulnerability they can find to gain access to a system and unpatched software is a common avenue to utilize. Most small to mid-size companies do not have a robust automated system in place to apply all the necessary operating system and software application patches on a regular basis. Without an automated patch management system, the duty falls on users and their individual systems to alert them to a patch that needs to be installed. Then, inevitably, when prompted to download the patch, an employee is in the middle of a task and clicks the "remind me later" button. (They may also fear that the patch itself is malicious. Either way, that patch is soon forgotten.) That's why having an automated patch management system in place can greatly enhance your security posture.

6. Exposed Sensitive Data

There have been several high-profile breaches in which the compromised data was not previously encrypted "at rest" (while being stored). Because of this, cybercriminals were able to access the data much more easily. Unfortunately, many corporations believe it's too costly or cumbersome to deploy encryption technology, when in reality, it's not. (Remember that a breach is way more expensive!) Encrypting your most sensitive data at rest can significantly reduce your risk of data loss, even if the adversary gains access to your systems and data. Several of the organizations in these well-publicized cases were also victimized because of poor configuration of network resources, which allowed valuable corporate systems to be internet facing and, thus, available for anyone to see. Leaving a sensitive system with a weak connection protocol, such as Microsoft's remote desktop protocol (RDP), can be a tremendous security risk. Luckily,



Unauthorized use of cloud applications…can be a nightmare for the company if access to those systems is exploited.

annual vulnerability assessments can uncover the critical systems and data in your network that are vulnerable to this type of attack.

7. Cloud Services

Cloud-based services, such as Dropbox and Google Drive, have made it easy to share sensitive corporate data with employees, clients, vendors, suppliers, and other partners. Unauthorized use of cloud applications, software, external hard drives, and mobile devices might make life easier for these groups, but it can be a nightmare for the company if access to those systems is exploited. In addition, the use of personal cloud-based backup services like Apple iCloud can significantly co-mingle sensitive corporate data with personal data. When an employee uses a personal device that has access to corporate data and uses iCloud backup services, a significant amount of the data is being backed up to that employee's personal account. Just because it's in the cloud, doesn't mean it's safe from cybercriminals.

Think it's time you did something about your company's security vulnerabilities? Avalon Cyber can help protect your company's data through the following proactive and reactive services:

Security Assessments

- **Vulnerability Assessments** – Our experts conduct internal and/or external scans to identify vulnerabilities and basic misconfigurations in your company's environment. Our team provides a comprehensive report and works with you every step of the way to develop a plan to address the most critical weaknesses and provide insights into the best way to implement improvements.
- **Penetration Tests** – Avalon Cyber team members safely simulate the actions of a cybercriminal targeting your network and attempt to exploit critical systems to access sensitive data. Penetration testing validates the efficiency of your currently deployed security resources and determines how well IT teams are implementing controls and whether employees are following existing security policies.
- **M365 best practices security audit** – We assess your current security settings and policies and identify where improvements

can be made to protect your instance and sensitive and business-critical data.

- **Firewall configuration review** – Our experts analyze firewall rules to determine whether security risks exist in the configuration and ensure security best practices are being followed.

Managed Detection and Response (MDR)

Our KnightVision MDR service is a robust endpoint monitoring solution that screens malicious behavior at the endpoint level, allowing our team of experts to alert you and take immediate action to shut down a potential threat.

Security Awareness Training & Phishing Simulation

No matter what size your business, training your team to recognize phishing attempts is a crucial addition to your security plan. Get them to think of emails as weapons because in the cyber world, they are. You want everyone from your C-suite to part-time workers to vendors on the same page when it comes to phishing and security.

Avalon Cyber and our partner KnowBe4, the world's largest security awareness training and simulated phishing platform, offer an innovative program that allows your security team to launch best-in-class, fully automated simulated phishing attacks and run comprehensive security awareness training campaigns to help educate your employees and stakeholders.

It's important to run these tests and training programs regularly to keep security top of mind and to test using the most up-to-date phishing attack methods. We even offer a free phishing security test if you'd like to see how your company fares against phishing lures.

Security Advisory Services

- **Policy Development** – Our experts can help you create or mature policies, procedures, and audit evidence needed to confirm controls are designed and operating effectively. Having a written record of what is required and how to proceed to meet those requirements ensures that everyone knows exactly what is needed to stay in compliance and keep your data safe.
- **Information Governance** – Avalon Cyber can help you develop project plans, identify necessary controls and processes,

If you **experience a cyber incident,** it's critical that you quickly **find and fill the gaps** in your network and **identify what data may have been compromised.**

and perform a readiness assessment around administrative, technical, and physical components of your program to identify effective policies and controls, as well as gaps. This will allow your organization to see its baseline compliance within a given framework and associated recommendations. In addition, our approach allows for evaluation of the internal and external controls that your organization employs and helps you identify a prioritized list of risks. By performing a risk assessment of people, processes, and technology, you gain an increased awareness of your organization, reduce the chances of a breach, and avoid regulatory issues.

SIEM and Managed SOC

Our KnightVision CAM (which stands for Compliance, Alerting, and Monitoring) combines a Security Information and Event Management (SIEM) platform, which collects, aggregates, and analyzes security event log data, and a managed Security Operations Center (SOC), i.e., a team of cybersecurity experts who respond to detected threats immediately. It's Avalon Cyber's customizable, scalable, affordable solution that addresses a range of cybersecurity challenges, including regulatory compliance, threat detection, and incident response.

Incident Response

If you experience a cyber incident, it's critical that you quickly find and fill the gaps in your network and identify what data may have been compromised. This process is a true forensic analysis process that traditional IT companies don't necessarily have the capacity for. The Avalon Cyber team has extensive experience in digital forensics and incident response and provide prompt and comprehensive response to cyberattacks. Our experts know where to find critical electronic evidence, and concurrently preserve and analyze it using today's most sophisticated digital forensic techniques and software. Avalon Cyber also offers assistance with data breach review and data breach notifications.

Incident Response (IR) Planning

Just as you run fire drills to keep your employees safe, your company should also practice managing security breaches together. Avalon Cyber's incident response planning service helps you identify, protect against, detect, respond to, and recover from a cyber incident. Our

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

team can guide you through plan creation and tabletop exercises, in which we run through various threat scenarios and practice how you would respond to those threats. We can also help you implement tools and technology to manage and mitigate security incidents. Remember, since threats constantly change, your IR plan will need to be modified and tested regularly. To further assist you, we offer an IR retainer program that allows you to have a cyber team on call 24/7/365.

vCISO

In this type of engagement, Avalon Cyber steps into the role of a virtual chief information security officer (vCISO) for companies that do not have the need or means to hire and pay for a full-time resource. Typically, this hybrid approach includes a few hours every month in which our experts become an extension of your team and provide support by overseeing the design, development, and integration of your cybersecurity program.

About Avalon Cyber

With decades of experience in the domains of digital forensics, cybersecurity incident response, IT risk management, and enterprise information security leadership, Avalon Cyber is the premier solution provider for cybersecurity and incident response services.

Our professionals have been conducting digital forensic and cyber incident response engagements since the early 2000s and have a deep understanding of adversary behaviors and their ever-evolving tools, tactics, and techniques used to compromise networks. The team members who support our managed security services have extensive experience in information security and possess industry certifications including: CISSP, OSCP, GPEN, CISM, CISA, CCNA, CCE, CFCE, EnCE, ACE, GXPN, OSCE, GSEC, ECIH, SSCP, CCSFP, and SEC+.

Avalon Cyber works with organizations looking to partner with experts to achieve a greater level of data security.