venio systems

Cybersecurity: 6 Keys to Keeping Your Data Secure

Introduction

Cybersecurity isn't a new concept. Ever since Robert Morris unleashed the world's first computer worm in 1988, the need to secure valuable computing resources has been readily apparent. But that need hasn't remained static. As more people and companies move more information and business to internet-accessible systems, the potential gains from computer malfeasance draw more attackers. Today's attackers are more malicious and more sophisticated than ever before and this change necessitates a commensurately more mature security response.

The threat landscape for digital systems is changing daily, and attackers only grow more bold. If you follow the news, you're likely aware of a major new wave in cybersecurity threats: ransomware. Ransomware is a type of attack in which a group of hackers exploit a system and encrypt all of the files on the system. They hold the key to decrypting the files and offer to do so for a fee. The rise of popular cryptocurrencies has fueled the growth in ransomware attacks around the world.

More significantly, the apparent success of ransomware attacks has emboldened attackers. Instead of targeting technically-challenged individuals, attackers have moved to targeting entire businesses and even sovereign nations.

This pattern tracks with the overall motion we've seen in the cybersecurity world. Attackers know the paydays they might score are astronomical and the risks of getting caught shrink in comparison. In May of 2020, a notable entertainment law firm, Grubman Shire Meiselas & Sacks (GSMS), was victim to a vicious ransomware attack by the REvil group, an infamous cybercriminal gang. A total of 756 gigabytes of contracts, nondisclosure agreements, personal and professional correspondences, and more data types were stolen from the company representing high profile clients, such as Lady Gaga, Madonna, Bruce Springsteen, Mary J. Blige, Nicki Minaj and many others. The ransom was initially set at $21 million, however, when it was revealed the company held sensitive information about the former US president, REvil upped the ransom to $42 million.

At Venio Systems, we're working hard to ensure your eDiscovery is secure by identifying the six most harmful vectors of cybersecurity, namely:

- People
- Policies and Procedures
- Data
- On-Premise
- Cloud
- Application

As we move through this whitepaper, we're going to discuss how attackers leverage these vectors to infiltrate organizations and how your eDiscovery vendor should secure each one to determine your overall mitigation strategy against cybersecurity threats.

First up, we'll talk about people and how your most important asset is also your most vulnerable.

Vector 1: People

There's an old cybersecurity truism that says securing a computer is easy; unplug it, bury it six feet underground, and never let anyone use it.

Unfortunately, eDiscovery depends on computers, and most computer systems have human interaction touchpoints somewhere along the processes they support. Whether that's processing human-generated data, interacting with people to achieve goals, or providing data to human beings for analysis, computers are there to support your human employees.

This is why people are such a valuable vector of invasion for malicious users who threaten your security. Think about what's easier: infiltrating a computer system, evading detection, and extracting some valuable data? Or gaining the trust of an employee and asking them to print out the data under the guise that you have legitimate access?

Attackers use techniques like phishing to gain the confidence of an existing employee and use that confidence as a way to proceed to the next step of their plan. Sometimes, this means getting the employee to turn over sensitive information, like passwords or internal company data. Other times, they use it as a launching point to compromise another employee with access to the systems or data they really want.

They might, for instance, ask an employee to install some software that appears useful, but really contains malicious code that gives the attacker access to internal company networks.

One popular, low-touch phishing attack involves leaving a few USB flash drives in the parking lot of a company that the attacker wants to compromise. From there, all they have to do is wait. They hope that an employee will pick up the flash drive and plug it into a company machine where it will automatically install malicious software so they can proceed to the next part of their attack.

The vast majority of cybersecurity breaches involve some kind of human error or intervention at some point in the process. So, how do you combat this? Unfortunately, there isn't a silver bullet for making sure your people aren't a security vulnerability. Like we noted above, the only fully secured system is one that nobody ever uses.

But you can take preventive steps. One key step is ensuring employees are aware of potential attack vectors and that they are trained in recognizing the signs of someone attempting to compromise the company through them. Another is ensuring you only provide employees access to information and systems that they need to access in order to do their job. It's also a good idea to take forensic steps—like logging all access to data (sensitive or not) and systems—so that way, in the event that you experience a cybersecurity incident, you're able to reconstruct the event in detail.

Vector 2: Policies and Procedures

A second vulnerable vector is the way your organization handles processes. Like we noted before, humans are the most vulnerable vector in IT security, and the way that humans carry out their work is the second-most vulnerable.

One key way to educate employees on the importance of security is through cybersecurity policies. A good policy explains the responsibilities of each employee in protecting IT systems and data. Cybersecurity policies set the standards of behavior for activities, like encrypting email attachments and restricting the use of social media.

Effective IT security policies reflect a vendor's culture. Rules and procedures derive from employee approaches to their information and work. The objectives of IT security policies are the preservation of confidentiality, integrity, and availability of systems and information used by a vendor's customers.

An information security policy aims to enact protections and limit the distribution of data to only those with authorized access and must contain guidelines about:

- Authority and access controls
- Data classification
- Security awareness training
- Responsibilities and duties of employees
- Virus protection procedures
- Malware protection procedures
- Network intrusion detection procedures

- Remote work procedures
- Technical guidelines
- Consequences for non-compliance
- Physical security requirements; and
- References to supporting documents

Another way to improve your overall security position is to invest in an eDiscovery vendor that complies with security regulations, like through System and Organization Controls (SOC) II certification. SOC II certified vendors, like Venio Systems, specialize in developing cloud-based software that meets the standards of the American Institute of Certified Public Accountants (AICPA) to ensure a vendor has controls in place to protect against unauthorized system or data access.

Vector 3: Data

Your data is one of your most important business assets. You want data to be available to the people who need it, whenever they need it, wherever they need it. This need is at tension with the need to safeguard your data from those who shouldn't have access to it.

Managing your organization's data in all its forms is a key aspect to securing your eDiscovery. Step one in organizing your data is understanding just what data you have and where it lives. Once you know where your data lives and how it moves, the next step is identifying who has access to it. Like we said, you want the people who need access to data to have it immediately, but the people who shouldn't have access to never see it at all. Too many organizations experience data leaks when they leave sensitive data visible to anyone within the organization.

Data isn't only at risk when someone accesses it or it passes between services. Malicious users will also attempt to compromise data when it's at rest. For instance, an attacker might have a hard time compromising your database password. They might have a much easier time getting access to the data stored in your database while it rests on a hard drive.

Your data lives a lot of lives. It's up to you to think about all of those different lives, and which eDiscovery vendor will secure your data in each phase of its existence. Often, your data is what attackers want the most; whether that's because it's sensitive on its own, like financial information or medical data, or because it allows them leverage over your business. Either way, you need to focus your efforts on securing your data at every turn.

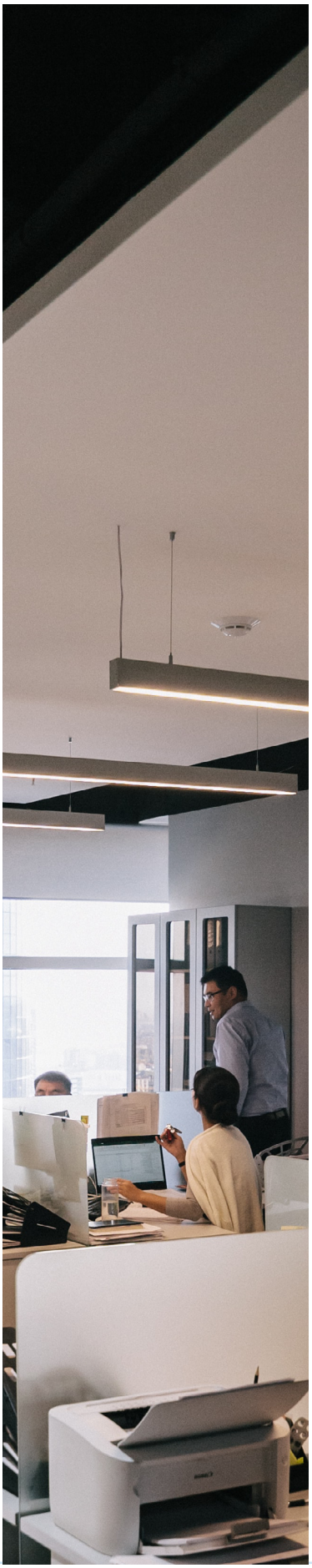
Vector 4: On-Premise

In an organization, the infrastructure typically resides on premise—either in one location, or many remote branches with security distributed accordingly. Keeping a local server has a few advantages, such as increased control over critical data.

However, inflexible IT budgets can make it difficult to develop the security expertise required to keep your business' data secure. On-premise security requires a substantial investment. Maintaining physical servers includes added operational costs, system upgrades, cooling kits, power delivery tools and costs, and more.

Regardless of the preventative measures organizations have in place for their on-premise infrastructures, data breaches and disruptive outages are still possible. Organizations are moving from conventional systems that were guarded with tight physical security to internet-connected systems with open infrastructures.

As the connectivity multiplies manifold, the systems are exposed and susceptible to destructive cyber threats. Thus, eDiscovery vendors must be able to quickly react to newly discovered vulnerabilities and significant system outages at the earliest possible time.



In order to impede cyber attackers, your eDiscovery vendor should make sure that they're employing the following key security postures:

- Encrypt all data at rest so that if any attacker were to gain access to your data, it would not be readable.
- Eliminate SQL injection vectors, to avoid attackers retrieving or corrupting data.
- Avoid query timeout issues, so that attackers cannot use them to clog up server performance.
- Change the default SQL server password, so that attackers cannot gain access to the system.
- Ensure that all servers are up to date with the latest Operating System and Software patches to avoid known vulnerabilities

Vector 5: Cloud

Adopting cloud computing infrastructure for your eDiscovery can complicate its cybersecurity. Because cloud services are managed by your eDiscovery vendor, you no longer control physical access to your computing resources and need to trust that your eDiscovery vendor is following security best practices at all times.

To ensure that your eDiscovery vendor keeps your data stored on the cloud as secure as possible, you should verify that they provide all of the following security features:

- VPN-only access, to ensure that people who are not on approved networks cannot access the eDiscovery software.
- No shared database architecture. Each client's data is stored in a distinct database to protect from one client gaining access to another's data.
- Incremental backups and disaster recovery failover servers ready at a moment's notice.
- Network and Security monitoring, to detect any intruders before they cause damage.
- Regular Penetration Testing and Security Vulnerability Scanning

Cyberattacks evolve with innovative, new approaches for seeding malware and stealing data that continue to disrupt cloud operations. Your eDiscovery vendor must, in turn, actively work to impede cyber spies, attackers and terrorists through a collaborative security approach that leverages analytics of data within the cloud.

Vector 6: Application

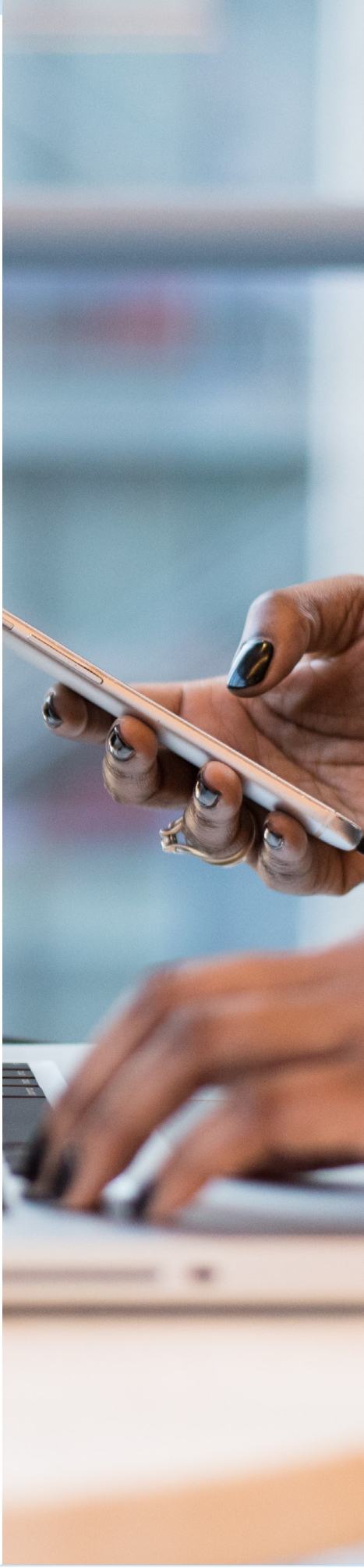
Often, if an attacker is looking to compromise a specific business, application security is the last vector they will seek to exploit. Application security refers to security built into the application, such as password protection and role based access control (RBAC) to manage who has access to your data.

A savvy attacker will do everything they can to find your flaws before they ever think about launching an attack. That includes leveraging your current or previous employees to root out information that isn't public knowledge. So, it's a great idea to consider how they will find their way into your application.

It's important to understand the software your organization uses, how it might expose your organization to risks posed by malicious actors, and most importantly, how your eDiscovery vendor implements security into their application to keep your data safe.

A quality eDiscovery application will implement all of the following application security features, and more:

- 2 Factor Authentication - strongly authenticate users when they log in.
- Role-based access control - only users who need access to a piece of data to do their job should be able to access it
- Data encryption - both in transit and at rest, so that malicious users cannot peek into sensitive data no matter where they might access it.
- Secure external sharing of data using email-based tokens - allow trusted users outside the organization to access sensitive data, while protecting it from prying eyes.
- Time-restricted data sharing - create an expiration date for shared data, closing a common vector for data leakage.



Defense In Depth Is Key

Each of the vectors we discussed is only one way an attacker might try to compromise your business. It's important to understand that many impactful attacks aren't simply attacks on a single vector, but instead involve leveraging one vector to gain access to an insecure part of another vector. At each step of the way, the attacker gets closer to what they're really looking for.

That's why mature eDiscovery vendors, like Venio Systems, focus on defense in depth strategies. Venio can help you deploy robust eDiscovery security practices and tools to protect your on-premise software and hardware, stand-alone applications, integrated platforms, and data in the cloud. Our security experts are constantly enhancing our eDiscovery defensibility by implementing and configuring industry-recognized tools—including but not limited to those pertaining to data security, application security, identity & access, logging & monitoring, risk management, incident management, and awareness training—so you and your legal team are prepared to combat even the worst cyberattack and avoid court sanctions or penalties.

We have the breadth and depth of skills to transform security from a source of fear, risk, and complexity into a source of confidence, value, and competitive advantage. Strengthen your security posture and your competence to meet regulatory requirements today and schedule a demonstration with our top team members.

Experience how our solution works.

Request a Demo