2021 Edition

Whitepaper

Cloud Security: Top Threats and Key Defenses

Table of Contents

Introduction

Data breaches and ransomware attacks continue to plague organizations, from small businesses and town governments to multinational chains and national utilities. Despite considerable advancement in cybersecurity technologies, cybercrime has only become more sophisticated and costly to businesses.

Some numbers from the IBM/ Ponemon Institute's *2019 Cost of a Data Breach* report illustrate the scope of the problem:

- The average cost of a data breach has increased to nearly $4 million worldwide. For U.S. companies, it was $8 million, up from $7.35 million in 2017. The biggest cost factor was loss of business, which accounted for 36% of the total.
- It now takes 279 days for the average IT department to identify and fix a data breach: 206 days to identify a breach and another 73 days to contain it. That's up from 201 days in 2016 and 266 in 2018.
- Data breaches caused by cyberattack (not employee negligence) account for 51% of breaches in 2019, up from 42% in 2014.
- The chance of any organization suffering a data breach within two years was 29.6% in 2019, nearly one-third more than in 2014.

Data Breaches Cost Small Companies More:

According to the IBM/Ponemon 2019 Cost of a Data Breach, small companies shoulder a higher relative cost for a data breach than large organizations. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million or $204 per employee. Smaller organizations (500 to 1,000 employees) had an average cost of $2.65 million or $3,533 per head.

Effective cybersecurity is a huge challenge for IT organizations, especially those with hybrid and multicloud environments. In fact, most organizations today have a hybrid mix of legacy on-premises, public cloud, private cloud and collocated systems. These mixed environments require different security solutions.

Forrester's 2019 report, *Empower Your IT Teams with Security As A Service* found that nearly half of companies with multicloud environments consider security to be their top concern, yet almost a third said they lacked sufficient in-house security expertise to manage it. As a result, many IT departments have turned to managed security services providers (MSSPs) to improve the quality of their defenses, as well as reduce cost and increase the speed of cloud security implementation and deployment. MSSPs offer solutions such as firewalls, data encryption, intrusion detection, mobile security, security monitoring and vulnerability assessments.

The Cybercrime Economy

Whether a company's data is in the cloud or in a traditional corporate network, it's a target for cyberthieves who may sell it on the thriving black market of stolen data and malware tools.

Most of the buying and selling of malware and data occurs over the "Dark Web"--a network of Internet sites that are only accessible by using specific encryption software like Tor software. Thieves with limited technical expertise can buy pre-packaged malware and other exploits, rent a DDoS attack service for a couple hours or subscribe to a ransomware as a service. Anyone can launch a sophisticated cyberattack today.

The Dark Web also provides a ready market of stolen data. According to VPNOverview's "*In The Dark*," there are many Dark Web marketplaces selling stolen personal and financial data, including bank account balances and numbers, PayPal passwords, email addresses and other information. Criminals sell everything from medical records and bank cards to social media accounts and "databases full of consumer data". Authentic and forged passports are available as well. You can buy a Canadian passport for about $700 and a U.S. driver's license for $1,000 on the Dark Web.

Not all cybercrimes are done for money. Cyberattackers include terrorists, spies, "hacktivists" (like Anonymous) and industrial espionage/intellectual property thieves. However, organized criminal groups are the dominant force behind cybercrime. Organized gangs with profits from drug smuggling, financial fraud and money laundering are also investing in cybercrime.

Top Cybersecurity Threats

As cybersecurity technologies get better, cybercriminals devise new ways to evade them. The most sophisticated attackers leverage multiple tactics and hacking tools and execute their exploits in phases to avoid detection.

An increasingly common strategy is to use a trusted system tool or process that isn't subject to security scanning, such as Windows PowerShell, to run malicious scripts, display connected devices, identify and kill processes and other activities. Using a trusted process to run a script also ensures that no files are left behind for anti-malware programs to find. A fileless script or process may continue to run until the computer is rebooted. Microsoft's Remote Desktop Protocol (RDP) is another potential vulnerability that can be leveraged by hackers. RDP enables administrators to connect to remote computers over a network, such as the Internet. Insecure RDP connections are favored points of entry for hackers and allow them to take over the remote computer, upload files, open directories and execute programs at will.

Artificial intelligence is making it possible to create faster and more targeted cyberattacks. With AI, an attacker can analyze vast amounts of information in emails, social media profiles, corporate web sites and other sources to better identify targets. AI can "learn" a victim's IT environment to find the best vulnerabilities to exploit or customize a phishing email to ensure the recipient opens it.

AI is behind the rise of *deepfakes*-- forged images, videos and audio that look and sound authentic. An audio deepfake, for example, can impersonate the voice of a business executive or other authorized end-user to trick voice recognition security or convince an IT administrator to provide a password. An attacker may order an employee to transfer funds or email sensitive files. *Trend Micro's security predictions for 2020* warns of increasingly sophisticated AI forgeries aimed at C-suite executives. *Forbes* wrote about one instance in which an energy company lost $243,000 to a scammer who faked the CEO's voice to order a money transfer. Security software firm *McAfee predicts* that deepfakes will be used to bypass facial recognition, presenting a significant security threat to businesses.

Many of the current cyberattacks, however, are based on tried-and-true methods, albeit with more sophisticated technologies and tactics.

The following are the main cyberattacks that threaten every organization:

Brute Force Attacks.
Sometimes referred to as "kicking down the door," a brute force attack uses automated tools to quickly gain access or steal data. One type of brute force attack is password hacking. A hacker uses a tool to quickly run hundreds of password combinations until one works. The weaker the user's password, the quicker it can be hacked. Another method is to plant keyword logging malware on a client. Any hacked account can be used to gain access to resources, but the riskiest accounts are those of superusers and administrators. Both of these types of users will have extensive, high-level access to a variety of resources and

Choosing A Secure Cloud Services Provider

Cloud services providers vary in their levels of expertise and capabilities. There are large national providers with financial stability and solid security as well as smaller local and regional providers with a variety of track records and expertise.

To determine a provider's security, **check their third-party security audits and proof of certifications**. While not all regional providers may have undergone a third-party audit, all should be able to show proof of having achieved IT security certifications.

Look for **proof of compliance** with industry and government regulations and standards, especially those relevant to your company's industry. Those might include:

- **NIST SP 800-53**
- **Service Organization Control (SOC) 1,2 or 3**
- **Control Objectives for Information and Related Technologies (COBIT)**
- **Federal Information Security Management Act (FISMA)**
- **Health Insurance Portability and Accountability (HIPAA)**
- **Gramm-Leach-Bliley Act (GLBA)**
- **Payment Card Industry Data Security Standard (PCI DSS)**
- **Sarbanes-Oxley Act (SOX)**
- **Other international security standards**

Also, a provider's staff should demonstrate their competence with professional certifications such as CompTIA Security, Certified Information Systems Security Professional or Certified Cloud Security Professional.

should have the strongest passwords.

Site scraping or data harvesting is another type of brute force attack. A bot or web crawler copies data and content from a site to use for malicious purposes such as creating a replica site, monitoring competitors' products and prices, or compiling lists of potential victims for phishing scams and identity theft.

Business Email Compromise (BEC).
This "man in the middle" caper typically involves a combination of email hacking, social engineering, faked domains and, in some cases, AI. A cybercrime committed in 2019 against a *Chinese venture capital firm* is a classic example. The scammers diverted $1 million from the Chinese firm, intended for an Israeli startup, into the scammers' own bank accounts. They did this by infiltrating the email accounts of both companies and sending forged emails with new bank account numbers to use for the pending deposit. A BEC scam works best when the victims are in different countries, communicate rarely and have no backup methods for authenticating orders. The target victims are typically financial executives or others with the authority to transfer funds.

Cloud API Vulnerabilities.
Application programming interfaces (APIs) provide developers—and hackers—with control over a cloud application. Developers use them for cloud services integration, management, monitoring and provisioning. Hackers can use an API to access sensitive data or reconfigure an application.

Unfortunately, APIs are often overlooked when it comes to security and may have inadequate authentication and encryption, logic flaws or other weaknesses. A poorly constructed API can enable a variety of attacks that can enable hackers to modify or steal data or other content.

McAfee Lab's predicts that vulnerable cloud APIs will be prime targets of hackers in the future, pointing to an Imperva survey that reported 68.8% of organizations exposed their APIs to the public. To avoid becoming the weak link in cybersecurity, cloud services API development will need to incorporate more of the security processes used in application development -- authorization, authentication, audit trails, identity management and encryption.

Distributed Denial of Service (DDoS).
A DDoS attack is a flood of junk traffic aimed at a network or IT server and intended to overwhelm the system. The traffic is typically generated by a botnet of infected computers or Internet devices. Depending on the type of DDoS attack, it might disable or damage a company's website or ecommerce site, application services and communications, or even its hardware.

There are five major types of DDoS attacks to guard against. These are:

- Advanced Persistent DoS (APDoS). An APDoS attack is a massive attack that may persist for weeks. It usually starts with a network-layer DDoS attack and application layer (HTTP) floods, followed by repeated SQLI and XSS attacks.

- DNS NXDOMAIN Flood. This targets an organization's DNS servers with a flood of malicious DNS lookup requests.

- SSL-based. These leverage encrypted traffic and may include encrypted SYN floods, SSL renegotiation, HTTPS floods or encrypted web application attacks.

- Permanent denial-of-service (PDoS). A PDoS exploit will damage a system so badly that it requires replacement of the hardware or firmware. By exploiting security flaws or misconfigurations, PDoS aims to destroy the basic functions of a system.

The growth of IoT devices has greatly enabled DDoS attackers. IoT devices are frequently unprotected and can easily be hijacked and used with thousands of other IoT devices to launch floods of DDoS traffic.

DNS Hijacking.
Symantec's *Internet Security Threat Report (ISTR) 2019* found that 1 in 10 URLs were malicious, up from one in 16 in 2017. Many of these malicious sites were created as part of a domain name server (DNS) hijacking campaign. A web site suffers a DNS hijack when its incoming traffic is rerouted a to different site. The motive of the hijacker might be to steal customers' credit card numbers, intercept data intended for the victim, alter email communications to defraud users or distribute malware as part of a multi-stage attack.

DNS hijacking may be done in different ways. One is to hack into the network of an organization that hosts a DNS--such a major ISP or telecommunications company—and change the IP address numbers of a target web site in the DNS. (A DNS ties IP address numbers to the URL name of a web site.) Another method is to upload malware directly onto the target's computer or router. The malware then redirects incoming traffic to the hijacker's site.

An example is *Sea Turtle*. In this multi-stage exploit, attackers broke into top level domain servers and altered the Internet addresses of multiple government-, military- and energy-related organizations. The hijackers were able to spy on the emails and web traffic of the target organizations.

Ransomware.
Europe's *Internet Organised Crime Threat Assessment (IOCTA)* named ransomware as the top threat that organizations faced in 2019, and it's not going to get any better. Ransomware is malware that encrypts the files on a computer or network and demands a ransom payment in exchange for the decryption key. It can be distributed through an infected email attachment, flash drive or a malicious website or planted on a system that was previously breached.

> ***Cybersecurity Ventures*** *predicts that a business will fall victim to a ransomware attack* ***every 14 seconds by 2019,*** *and* ***every 11 seconds by 2021.***

McAfee predicts a rise in secondary extortion attempts after the first ransomware demand. In a secondary attack, the hacker may use files or data exfiltrated prior to encrypting in the first wave to later threaten the victim. The attacker might threaten to publish or sell the information on the Dark Web unless the victim pays an additional fee. The stolen data may also be used as extra leverage to convince a reluctant victim to pay the first ransomware demand.

The most vulnerable victims tend to be smaller public or private organizations with limited IT resources. These organizations may be behind on security patches and upgrades or lack a disaster recovery process. Municipal governments are a frequent target. In one week in April 2019, a series of towns in Maine, California, Florida and North Carolina were hit with ransomware, forcing some to resort to paper forms and personal email accounts for days afterwards.

While ransoms can be high – average payment is $41,198 according to *Coveware* – the costs of data recovery plus the loss of business are usually much higher. Baltimore is a good example. An attack in 2019 cost the city an estimated $10 million.

In some cases, an attack can force a business to close its doors. The Wood Ranch Medical clinic in Simi Valley, CA was infected with ransomware that encrypted patients' files. The clinic's owner opted to close shop four months later, citing the cost and time it would take to recover.

Paying ransom does not guarantee the data will be restored. Often, the attacker either takes the money but doesn't send the decryption key or the key doesn't work. Also, some types of ransomware are designed to make data unrecoverable.

Remote Access Trojans.
A growing threat to companies is the RAT—the *remote access trojan*. According to Cisco's *Threats of the Year 2019*, RATs will multiply in 2020. A RAT is malware that gives a hacker remote access to a system. An example is SDBbot which, once installed gathers data on the users and their IT systems, and then establishes a connection between the victim's and hacker's servers.

Like any "trojan" malware, a RAT is designed to evade security by disguising itself as something innocent, such as a game app or email attachment from a co-worker. Once inside, the RAT provides a command line interface to remotely control the victim's system. An attacker can access administrative tools, change or delete files, kill processes or install more malware. The RAT might log keystrokes or turn on the computer's microphone. In fact, with a RAT, a hacker can do pretty much anything he wants to on your system.

Spyware.
While not necessarily as dangerous as ransomware and DDoS, spyware can be highly damaging. Like the name implies, spyware helps hackers learn more about your business operations, your IT infrastructure and employee computing practices. Hackers can use that information to create more effective malware, to understand where your most valuable data lies and how to get at it, or to sell it to other hackers looking for lucrative corporate assets to attack.

Spyware often masquerades as a freeware utility or game for users to download onto network clients or mobile devices. It may also look for vulnerabilities in applications. A flaw in Facebook's WhatsApp messaging service in 2019 enabled spyware created for the Israeli intelligence services to infect users' phones. According to *Fighting Identity Crimes*, the spyware allowed hackers to spy on WhatsApp users through their phone's camera and microphone.

Web Application Attacks.
These exploit vulnerabilities in web browsers and application components. The goal may be to execute a malicious script, upload malware, gain access to a backend server or to steal credit card numbers.

An example is *form jacking* or the insertion of malicious code into a web page, such as the payment page on an ecommerce site. Two other common ones are cross-site scripting and SQL injection, both of which insert malicious code into a web page input field.

Cross-site scripting attacks input scripts into a web site's contact form. The script executes when someone opens the message. The goal might be to hijack a user's session, post messages on their behalf, capture keystrokes or do other activities.

A *SQL injection* targets a web site's database. The attacker inputs malicious SQL code into the query page, either to infiltrate back-end systems or to infect the browsers of web site visitors.

Cloud Defense in Depth

Multiple threats demand multiple defenses. An in-depth security strategy for a hybrid IT environment will have multiple types of security solutions aimed at thwarting specific threats to both cloud and on-premises systems. The types of defensive security services that your hybrid IT environment should have include the following:

Next-Generation Firewalls.
Traditional firewalls are no match for today's sophisticated attacks. These traditional firewalls mostly provided basic packet and URL filtering, but didn't really address intrusions, sophisticated malware, nefarious websites, phishing emails, and web application attacks – without additional security measures put in place separately. Next-generation firewalls are designed to defend against multiple types of cybersecurity threats, while being managed and monitored through

Factors that reduced data breach losses

IBM/Ponemon 2019 Cost of Data Breach found **several factors that reduce the cost of a breach**. Automated IT security systems are one of the most crucial factors in cost reduction.

Organizations that lack fully deployed security automation suffer 95% higher losses than those with automated and deployed security solutions: $5.16 million average total cost of a breach without automation vs. $2.65 million with automated security.

Other important factors in decreasing costs include encryption, data loss prevention and threat intelligence sharing. **Encryption reduces breach costs by an average of $360,000.**

After a breach occurs, an organization can mitigate losses by having an incident response (IR) plan and by implementing a business continuity/disaster recovery plan. Those with frequently tested IR plans had average total cost that was $1.23 million less than those that no plan. **Business continuity management in the aftermath of a breach reduced the total cost of a data breach by an average of $280,000.**

one single interface. They offer a far easier solution than a piecemeal collection of standalone security products.

In addition, most provide the ability to activate the different security features as needed, so an organization can start with basic traffic monitoring and add capabilities when ready. Some of the big benefits of next-generation firewalls are web application vulnerability patching and DDoS mitigation, content filtering to block web pages and e-mails that violate company policy, support for VPNs with multi-factor authentication, SSL inspection of encrypted content, and regularly updated threat intelligence for IP reputation and malware signature filtering.

Intrusion Detection and Prevention Services (IDPS).
Cloud IDPS detects and identifies potential threats and then blocks them.

The detection component of IDPS scans for a variety of threats including malware, phishing attempts and network attacks. IDPS conducts basic scanning for known threats using databases of existing threat signatures to compare against possible incoming attacks or malware. IDPS also scans for new threats, not yet in the database, by continuously monitoring both end-users and applications for irregular activity, such as sudden spikes in traffic that might indicate a DDoS attack or multiple login attempts that could indicate password hacking. This intelligent monitoring can help detect zero-day attacks.

To prevent threats from infecting or breaching the network, IDPS blocks malicious traffic and malware, as well as enforces application and network protocols. IP packets or transmissions from suspect IP addresses are blocked or dropped.

Web Application Firewall (WAF).
A web application firewall is a hardware appliance or cloud solution that inspects incoming HTTP and HTTPS traffic for indications of malicious activity. A WAF is specifically designed to block web application attacks such as cross-site scripting, SQL injection, and other attacks designed to take advantage of application or browser vulnerabilities.

A WAF with botnet detection and mitigation capabilities can also block site scrapers that automatically roam the Internet collecting data from web sites, such as pricing data or executive names. Bot detection can be done via HTML header inspection and the reputation of the IP address, visual challenges such as CAPTCHA recognition, or other techniques.

A web application firewall also provides protection from third-party software bugs and zero-day vulnerabilities.

Microsegmentation.
Microsegmentation is the process of using software to assign network security policies or zones to each of your workloads (in a data center or cloud) rather than a blanket network security policy – allowing for a more granular control over workload security and reducing the network's attack surface (making it much harder for intruders to access multiple workloads). This approach provides stronger security as you create security policies dedicated solely for your different workloads.

Identity Access Management (IAM) and Multi-Factor Authentication.
Identity access applications help enforce "need to access" policies on all data and content. They also help prevent dormant accounts from being hijacked. IAM and IDaaS provide user authentication and role-based access management to ensure that anyone opening or copying a file or accessing an application is authorized to do so. Assigned roles based on seniority or work activities may specify which resources an end-user can access and what actions they can take.

Identity management applications can block unauthorized users from accessing content or applications and selectively prevent other users from accessing resources that are outside of their assigned roles. For example, an editor may be allowed to download, open, edit and save editorial documents, but not departmental budgets or payroll records. A sales employee might be allowed to access her own sales goals but not those of her coworkers.

IAM and IDaaS include functions such as automatic deprovisioning of old accounts, reviewing user privileges, enabling self-service for simple user requests such as password resets, and other administrative functions.

Gartner reports that by 2022, 60% of access management applications will incorporate user and entity (e.g. client) behavior analytics capabilities and other features for continuous authentication, authorization and online fraud detection.

Like identity access management applications, multi-factor authentication is essential for protecting sensitive data. Multi-factor authentication requires a user to have two, but preferably three, types of identification to access an account, making it harder to steal account credentials. Those types of identification would typically include a password, PIN, USB token, random password generator, or a biometric scan of a fingerprint or retina. Multi-factor authentication is often part of an identity access management service.

Endpoint & Encryption Protection. Endpoint antimalware or antivirus software scans files on endpoints such as PCs, flash drives and email servers before those files are uploaded or copied to a computer on the corporate network. This prevents malicious apps, like ransomware, from sneaking into the network.

Endpoint security software can also determine whether a company file can be downloaded onto an endpoint. This protects sensitive files from being copied onto removable drives or cell phones. Controls enable administrators to set policies for the types of files or data that can be copied or shared and under what circumstances. Controls also allow administrators to configure endpoints, pushing out updates and enforce usage policies.

> *Many CIOs also partner with **Managed Security Services Providers (MSSPs)** who can select, implement and manage security solutions that are optimal for different IT environments.*

Encryption software keeps unauthorized users from accessing applications and data. There are two main types of encryption, device-based and file-based. When a device is encrypted, the contents cannot be accessed without the decryption key. This ensures that the hardware is protected from malicious actors with physical access to a device. File-based encryption protects individual files and those files also cannot be accessed without the decryption key.

Combining endpoint protection and encryption is a strong line of defense against those looking to corrupt or steal files, install malware, and access applications without authorization.

Cloud Security: A Shared Responsibility

A common assumption by many customers of cloud services is that the cloud provider is responsible for security. In fact, in-depth security requires vigilance from both provider and customer. An SLA will define each party's responsibility but, usually, cloud providers secure the services that they supply. A software-as-a-service provider will provide security for the software, as well as the underlying platform and infrastructure. A platform-as-a-service provider secures the platform and infrastructure, but the customer is responsible for securing any applications it deploys on the platform. In all cases, the customer is responsible for its own data and may want to augment the cloud provider's security as well.

Many CIOs also partner with managed security services providers (MSSPs) who can select, implement and manage security solutions that are optimal for different IT environments. For companies with complex, hybrid IT systems, an MSSP can quickly assemble the right security solutions.

An MSSP can also alleviate the shortage of IT security professionals. A lack of experienced security staff can leave an organization vulnerable to cyberattack. Large MSSPs and

CSPs with multiple regional and national data centers have security expertise and technologies to identify and block threats quickly, as well as the extra bandwidth to help absorb an initial DDoS attack.

As the volume of cybercrimes continues to grow, few individual businesses will be able to affordably guarantee the security of their data and IT resources without the help of outside security experts and cloud security services.

tierpoint®

Learn more about how TierPoint can help you with your Cloud Security.

Contact us today.

Call: 877.859.TIER (8437)
E-mail: sales@tierpoint.com
Visit: tierpoint.com

About TierPoint

A leading national provider of hybrid IT solutions, TierPoint helps organizations drive performance and manage risk. No U.S. provider comes close to matching TierPoint's unique combination of thousands of clients; more than 40 edge-capable data centers and 8 multitenant cloud pods coast to coast; and a comprehensive portfolio of cloud solutions, colocation, disaster recovery, security and other managed IT services. With white-glove customer service, TierPoint professionals customize and manage agile solutions that address each client's unique needs.