Cybersecurity

PROTECT THE VALUE OF YOUR COMPANY
AN OVERVIEW

Cybersecurity, at its core, is about protecting what’s valuable to you as an organization. For some, that might mean protecting valuable customer data—credit card information, Social Security numbers, or patient health care records. For technology companies, it’s also about protecting intellectual property. This includes source code, designs, products, or future product strategies. Collectively, that intellectual property defines the value of a tech company, and that value is usually sitting on a server as an easy target to be hacked.

02 AN INCREASING THREAT
- Influencing Factors
- Accountability

07 ATTACK TYPES
- Phishing
- Ransomware
- Internet of Things

12 ASSESSING YOUR VULNERABILITIES
- Common Weaknesses
- Risk Assessment & Analysis
- Penetration Testing
- Third-Party Due Diligence

15 RECOVERING FROM AN ATTACK
For many organizations, it’s no longer a question of whether a network will be compromised but when a network will be compromised. Almost 50% of all companies experienced at least one security incident during a 12-month period, according to a 2017 survey by the Ponemon Institute. If that isn’t an impressive enough figure, then consider this: The average data breach costs a company $3.9 million.

That’s a frightening perspective with a huge cost attached to it—and things aren’t going to get better anytime soon.

**INFLUENCING FACTORS**

**Emerging Technology**

The rapid proliferation of new technology, including a wide array of mobile devices and cloud-based solutions, means that hackers now have many more entry points to attack.

**Universal Vulnerability**

Additional vigilance is required for larger companies because of their access to valuable information and pervasive technologies, which makes them a natural target. This doesn’t let the small guy off the hook, though. If there are rumblings that a start-up has the next killer app in development, for example, they’re vulnerable to attack.

**International Threats**

Economic espionage, or cyberespionage, isn’t limited to borders. It isn’t uncommon for overseas companies to target entities releasing products with high potential for profit and revenue. While the act itself isn’t necessarily something new, there are now organized and contracted teams leading the attack.

**Social Engineering Attacks**

Even with stronger security defenses, organizations are still at a disadvantage in the fight against hackers. Why? Because cyberattacks are increasingly aimed at individuals rather than systems—and the human factor is much harder to manage. People, however, are also the first line of defense with proper training.
CYBERATTACK EXAMPLES

**NOVEMBER 2017**
Uber had personal data for 57 million users and drivers worldwide stolen. The breach was compounded by a lack of transparency—the attack happened in October 2016 but wasn’t publicly announced for more than a year. Uber paid $100,000 to the hacker to destroy the data.

**JULY 2017**
Equifax was compromised after an attack left more than 143 million consumer records vulnerable. Those records included Social Security numbers, credit card information, and other identifiable personal data.

**FEBRUARY 2016**
Hollywood Presbyterian Medical Center paid a hacker $17,000 in bitcoin after a ransomware attack encrypted its electronic medical record system, effectively locking the hospital out of its records for a week.

**FEBRUARY 2015**
Intuit had to warn its TurboTax customers to hold off from filing tax returns to ensure hackers couldn’t steal their refunds.

**JANUARY 2015**
Anthem Blue Cross Insurance Companies, the nation’s second largest insurer, disclosed a breach in which the identities of 80 million customers were potentially stolen.

**NOVEMBER 2014**
Sony Pictures found that email systems were accessed and embarrassing discussions were made public with costly consequences.

**JULY–AUGUST 2014**
JPMorgan Chase discovered unauthorized individuals accessed more than 90 of its secure servers over a two-month period. The result was the loss of personal financial information for at least 76 million households.

**DECEMBER 2013**
Target had 70 million customer’s payment card transactions stolen.
ACCOUNTABILITY

High-profile enterprise hacking leads to the painful loss of precious data, customer confidence, and hundreds of millions of dollars in legal fees, notification costs, and technology remediation.

It’s no wonder C-level executives are now paying more attention to their organizations’ vulnerabilities when it comes to cybersecurity. Other individuals also demand results:

- Investors and boards of directors are increasingly holding senior management accountable for cybersecurity.
- Customers and partners demand adequate cybersecurity controls are in place before conducting business.
- US states, regulators, and regulatory bodies are legally mandating cybersecurity compliance.

Standards and Guidelines

Companies are also embracing new cybersecurity standards and guidelines.

- National Institute of Standards and Technology’s Cybersecurity Framework (NIST CSF)
- Special Publication 800-53, Revision 4 (NIST SP 800-53r4)
- International Standards Organization (ISO) 27001
- AICPA’s SOC for Cybersecurity
TOTAL COST OF A BREACH
BY NUMBER OF RECORDS STOLEN

<table>
<thead>
<tr>
<th>Number of Records Stolen</th>
<th>Cost ($M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 10,000</td>
<td>1.9</td>
</tr>
<tr>
<td>10,000–25,000</td>
<td>2.8</td>
</tr>
<tr>
<td>25,001–50,000</td>
<td>4.6</td>
</tr>
<tr>
<td>Greater than 50,000</td>
<td>6.3</td>
</tr>
<tr>
<td>AVERAGE</td>
<td>3.9</td>
</tr>
</tbody>
</table>

COST OF EACH RECORD HACKED
BY INDUSTRY

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost per Record (£)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>380</td>
</tr>
<tr>
<td>Financial</td>
<td>245</td>
</tr>
<tr>
<td>Services</td>
<td>223</td>
</tr>
<tr>
<td>Education</td>
<td>200</td>
</tr>
<tr>
<td>Life science</td>
<td>188</td>
</tr>
<tr>
<td>Technology</td>
<td>165</td>
</tr>
<tr>
<td>Retail</td>
<td>154</td>
</tr>
<tr>
<td>Communications</td>
<td>150</td>
</tr>
<tr>
<td>Industrial</td>
<td>149</td>
</tr>
<tr>
<td>Energy</td>
<td>137</td>
</tr>
<tr>
<td>Consumer</td>
<td>132</td>
</tr>
<tr>
<td>Entertainment</td>
<td>131</td>
</tr>
<tr>
<td>Hospitality</td>
<td>124</td>
</tr>
<tr>
<td>Transportation</td>
<td>123</td>
</tr>
<tr>
<td>Media</td>
<td>119</td>
</tr>
<tr>
<td>Research</td>
<td>101</td>
</tr>
<tr>
<td>Public Sector</td>
<td>71</td>
</tr>
<tr>
<td>AVERAGE</td>
<td>164</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute, 2017
It's no longer a question of whether a network will be compromised, but *when* a network will be compromised.

54%  
Companies that experienced one or more successful cyberattacks.  
Source: Ponemon Institute, 2017

$3.9 million  
Average cost a company pays for a data breach  
Source: Ponemon Institute, 2017

$600 billion  
Total cost of data breaches and cybercrime worldwide in 2017  
Source: Joint study by antivirus software maker McAfee and the Center for Strategic and International Studies
Attack Types

Attackers are increasingly sophisticated and have more access points to networks, including mobile phone devices. It’s important to remember that professionals typically hack people, they don’t go after the system.

Common Cyberattack Approaches

**Spear Phishing**
This is an email that asks for information—IT system access data or bank details—in the hopes of someone innocently responding and providing it.

**Whaling**
This method is the same as spear phishing but targets C-level executives.

**Ransomware**
Hackers gain access to a system using malicious software, then encrypt sensitive data and hold it hostage—along with your ability to conduct business—until a demand is satisfied.

**Internet of Things**
This includes many different types of devices that perform a single function at low processing power and lack security functions.

Attacks that began with spear phishing,

Mobile threats, specifically new mobile malware variants

Source: Symantec’s Internet Security Threat Report 2018
PHISHING

Spear Phishing

Sophisticated attacks usually begin here. A social engineering attack preys on the psychological willingness of employees to divulge a company’s confidential digital information.

These attacks involve an email from a hacker who appears to be an individual or business you know. The target tends to be an unaware or untrained employee who may be willing to give up desirable information—their system password or company account details, for example.

Whaling

When the target is C-level executives, it’s known as whaling. C-level email fraud takes place when a hacker requests that members of an organization’s finance function disburse or wire funds to a third-party in an email that looks like it comes from senior management. (See example to the right.)

Defense Strategy

It’s important to remember there isn’t an all-encompassing solution to combat spear phishing or whaling. Prior to an attack, these defenses should be in place:

End-User Security Training

Never forget that people are your first line of defense.

Technical Controls

This includes email system security, including antispam, URL scanning, and attachment stripping.

Internal Process Controls

Have at least two sets of eyes and approval for requests that meet a certain threshold.

WHALING EXAMPLE

In this example, someone named Mary is emailing Joe, the CFO of a company, to urgently request payment. What should Joe do?

Joe’s first step should be to slow down and think about the validity of a request when it comes in. He should take the time to hover over any hyperlinks to see where it’s going or check the email address carefully to be sure

Hi Joe

Mary CEO

February 29, 2018 at 10:44 AM
To: Joe.CFO@example.com

Hi Joe

Are you in the office? Kindly let me know because I need you to send out an important payment for me today.

Thank you,

Mary CEO

Sent from my iPhone
RANSOMWARE
Also known as scareware, this software allows hackers to access an employee’s computer, encrypt sensitive data, and then demand some form of payment to decrypt it. Often beginning with a spear-phishing attack, it infects the system and can propagate from there.

Defense Strategy
There are administrative and technical controls to employ in this situation.

Administrative Controls
• End-user security awareness training
• Internal process controls
• Disaster recovery and business continuity plans
• Contact information for local law enforcement, the FBI, and service providers

Technical Controls
• Frequent backups and snapshots of databases
• Test backups for key systems
• Network segmentation
• Up-to-date antivirus and system software through frequent patching
• Near real-time monitoring services, such as firewall information networks
While these figures are good reference points, it’s important to note that the price of data fluctuates frequently according to the market.

Source: Experian
INTERNET OF THINGS

Another entry point for hackers is the Internet of Things, or IoT. These devices—a wireless HVAC controller, smart watch, or even a drug-infusion pump that dispenses medication based on a patient’s physiological alerts—are particularly vulnerable because vendors are rushing to push products to market without considering the design of security elements.

Security and privacy are also hindered by the fact that a myriad of manufacturers have too many different types of devices, which typically have low processing power, are designed to perform a single function, and aren’t secured with universally accepted security standards.

Defense Strategy

- Know where IoT devices are in the environment
- Develop a policy for governing the use of IoT devices in the environment
- Have governance and risk assessment processes in place when new IoT devices are considered
- Use a separate wireless network to separate devices from the corporate network
- Use encryption while data is in transit, especially for sensitive information, if possible

OTHER EXAMPLES OF IOT DEVICES

- AVL sensor in a public transportation card
- Smart video conferencing systems
- Radio frequency identification (RFID) systems used for inventory
- Vending machines
- Fitbits

40.9 BILLION
2020 forecast for the number of devices, which is double the numbers from 2014.
Source: ABI Research

$7.1 TRILLION
IoT solutions will grow to this amount in the worldwide market from $1.9 trillion in 2013.
Source: International Data Corporation
## Assessing Your Vulnerabilities

### COMMON WEAKNESSES

A cybersecurity attack is often adapted for a particular company or industry. Here are five common problems that make organizations especially vulnerable to cyberattacks.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>01</strong></td>
<td><strong>EXCESSIVE ADMINISTRATOR-LEVEL ACCESS TO NETWORKS AND SYSTEMS</strong>&lt;br&gt; We’ve seen instances where vendors, consultants, and outside contractors retain access long after engagements with organizations are completed.</td>
</tr>
<tr>
<td><strong>02</strong></td>
<td><strong>EXCESSIVE PHYSICAL ACCESS TO DATA CENTERS AND SERVER ROOMS</strong>&lt;br&gt; In many cases, this broad-based access doesn’t have a business need and often leads to data breaches.</td>
</tr>
<tr>
<td><strong>03</strong></td>
<td><strong>GENERAL LACK OF CYBERSECURITY AWARENESS AMONG EXECUTIVES AND EMPLOYEES</strong>&lt;br&gt; Training is essential so that staff at all levels are aware of cybersecurity risks and how to recognize and avoid them. This training should be included in a mandatory HR best practices portfolio and conducted annually.</td>
</tr>
<tr>
<td><strong>04</strong></td>
<td><strong>INADEQUATE DISASTER RECOVERY PLAN</strong>&lt;br&gt; A proper plan should include steps to deal with destructive data loss or a security breach. A number of companies are ill-prepared to cope with this type of crisis, and the ensuing damage and recovery time can be exponential.</td>
</tr>
<tr>
<td><strong>05</strong></td>
<td><strong>PRIORITIZING CONVENIENCE</strong>&lt;br&gt; Too many organizations, especially smaller ones, choose convenience over high-level cybersecurity. For example, they have one flat network that doesn’t contribute to a layered defense rather than a segmented structure. This prevents a company from containing a security breach in one isolated part of the network.</td>
</tr>
</tbody>
</table>
RISK ASSESSMENT & ANALYSIS

There are many ways to infiltrate a company. Often, a company’s biggest weakness is not knowing how exposed it is to a cyberattack. An IT security risk assessment and analysis can help identify and assess the holes in your operation—a good first step toward protecting your organization.

A risk assessment can help answer several key questions:

• What systems are most at risk?
• Who has access to the most significant organizational data?
• How was mission-critical data acquired?
• What vital data is being processed, and how?
• What essential data is being stored, and how?
• What valuable data is being transmitted, and how?
• Where is crucial data being transmitted?

A cybersecurity risk assessment and analysis needs to be conducted annually and should focus on internal cybersecurity controls each year as well. It’s important to know what cybersecurity controls are installed as well as if those controls are working and up to date.

Examine these cybersecurity controls on a regular basis:

Administrative Security Controls
Policies and procedures related to IT security, incident response plans, and disaster recovery plans

Technology Controls
Networks, servers, mobile devices, and workstations

Physical Controls
Access rights to your data center and server rooms

Operational Controls
Approval processes

Social Engineering Controls
Confront the newest forms of people-driven cyberattacks through security awareness training
PENETRATION TESTING

In addition to conducting a cybersecurity risk assessment and analysis and focusing on internal cybersecurity controls, prudent cybersecurity management also requires penetration testing.

Penetration testing allows highly skilled and experienced security consultants to identify vulnerabilities by invading your systems from a cyberattacker’s perspective. Put another way, penetration testing is “ethical” hacking.

Among other things, penetration testing helps identify:

- Holes and flaws in IT systems
- Patches that were installed to fix issues
- Incorrect or inadequate configurations
- Updates and upgrades that have and haven’t been performed

THIRD-PARTY DUE DILIGENCE

If you use cloud-based or third-party hosting services or other services that help manage an aspect of your technology environment, such as firewall management or data backup, then you should ascertain the protections and security measures the vendor has in place to protect client data.

Audits: Attestation Reports on Controls

A company should request and review a Service Organization Control (SOC) examination report, also known as SSAE 18. Alternatively, utilize an ISO 27001 audit by an independent and objective firm that specializes in technology audits before entering into an agreement with the service provider and giving them access to your sensitive data.

In addition, the contract between your organization and the service provider should include language that allows you to conduct audits of their hosting environment.
Recovering from an Attack

If your organization does experience a data breach, there are immediate steps that should be taken to stem the damage and minimize the impact as well as to stay compliant with regulatory requirements.

01 Exercise Your Security Incident Response Plan
When a breach occurs, time is of the essence. Having an incident response plan is instrumental in alleviating the pressure of making decisions.

02 Bring In a Fresh Set of Eyes
This perspective often comes from a third-party that specializes in computer forensics or postattack analysis; the FBI has a division that investigates cybersecurity breaches, for example. The objective is to reveal clues or leads and offer external assistance when IT staff, who are often too close to the situation, might get weary-eyed and lose focus.

03 Know Your Notification Responsibilities
Federal and state-specific regulations mandate that affected parties be notified of any data breach that involves their personal information. It’s important to know what your organization’s obligations are from a compliance standpoint to avoid potential monetary penalties, fines, and lawsuits.

04 Call Your Insurance Carrier
Contact your insurance agent immediately upon stabilizing the situation. Determine what’s covered, which may include fees related to legal, public relations, communications, notifications to external parties, forensics activities, and the overall response effort. Also, determine if theft of proprietary information is covered, particularly if you have intellectual property.

A typical plan should include:
- Roles and responsibilities
- Trigger incidents
- Technology environment overview, including a network diagram, containment procedures, and eradication and cleanup procedures
- Communications protocols
- A call list, including key vendors the organization is dependent on for technology support

05 Develop Remediation Plans
After the situation has stabilized, many organizations fail to learn from their mistakes and don’t implement the controls or protections necessary to prevent a future attack or at least minimize the risk of a successful attack. Developing a remediation plan to address the risk and implement stronger controls and protections is essential to ensuring a similar attack doesn’t occur in the future.

06 Include Security Protocol and Controls in Your Business Processes
Practice securing data throughout its life cycle. This means considering protections and security controls that should be in place once the data is acquired, when it goes through processing, where it gets stored, and when it’s transmitted or moved.
Cybersecurity is a bit like playing cat and mouse. The risk of a breach will always be present, but staying one step ahead and being aware of evolving cybersecurity threats will go a long way toward enhancing your organization’s security.

If you’d like to learn more, contact your Moss Adams professional or visit us online.

mossadams.com/cybersecurity

CYBERSECURITY SERVICES

• IT security assessments
• Network vulnerability assessments and penetration testing
• Web application penetration testing
• Security analytics
• Wireless network assessments
• Social engineering
• Disaster recovery and business continuity planning
• Application code security reviews

PROFESSIONAL AFFILIATIONS

Our professionals are members of a number of information security associations, including:

• Information Systems Audit and Control Association
• Information Systems Security Association
• International Information Systems Security Certification Consortium
• Institute of Internal Auditors
• Cloud Security Alliance
The material appearing in this communication is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.
About Moss Adams

With 2,900 professionals across 25-plus locations in the West and beyond, Moss Adams provides the world’s most innovative companies with specialized accounting, consulting, and wealth management services to help them embrace emerging opportunity. Discover how Moss Adams is bringing more West to Business.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory services offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.