MOSSADAMS

Cybersecurity Best Practices for E-commerce Businesses

October 13, 2021

Presenters

Frank Kaufman, CPA
Retail National Practice Leader

(949) 933-9646
frank.kaufman@mossadams.com

Francis Tam
Partner, Cybersecurity

(310) 295-3852
francis.tam@mossadams.com

Bill Bussiere
Guest speaker

bill.bussiere@gmail.com

Agenda

01 Recent Cases & Trends

02 Guest Speaker: Bill Bussiere

03 Today’s Cybersecurity Environment

04 Best Practices

05 Q&A

POLLING QUESTION

Do you think your company is vulnerable to cyber attacks, such as malware, phishing, ransomware and other attacks?

A. My company is impenetrable

B. Not a concern as I have good cyber insurance

C. My company cybersecurity is average; a breach or not depends on my luck

D. My company has done something, but I am not sure

E. I have no idea

Industry Results

- Victims sustained $1.7B in losses due to business email compromises in 2019. FBI's Internet Crime Report 2020
- The average paid loss for a closed standalone cyber claim moved to $358,000 in 2020 from $145,000 in 2019. FitchRatings May 2021
- Industry statutory direct loss plus defense & cost containment ratio for standalone cyber insurance rose sharply to 73% in 2020 vs 42% for the previous Five Years (2015-1019). Fitch Rating May 2021
- Average downtime due to a ransomware attack is 19 days. 70% of ransomware attacks are aimed at organization with less than 1,000 employees. Coverware study 2021.
- Axis reported a 404% increase in ransomware demands from 2018 to 2019
- Beazley reported social engineering attacks increase 46% in Q1 2020 and 60% in Q2 2020
- Coalition reports most frequent types of losses were ransomware (41%), funds transfer fraud (27%) and business email compromise incidents (19%)

Largest Known Ransomware Payments

ORGANIZATION	AMOUNT	DATE
University of California at San Francisco	$1.14 million	June 2020
Travelex	$2.3 million	December 2019
Brenntag	$4.4 million	May 2021
Colonial Pipeline	$4.4 million	May 2021
CWT Global	$4.5 million	July 2020
JBS	$11.0 million	June 2021
CNA	$40.0 million	May 2021

Verizon Data Breach Investigations Report 2021

- Financially motivated attacks continue to be the most common.
- 89% of breaches occur through web application attacks.
- “In the same way automation may be helping you scale up your defensive operations, it can also help attackers scale up their offense.”
- “Actors are now exfiltrating the data they encrypt so that they can threated to reveal it publicly if the victim does not pay the ransom.”
- The middle 80% of breach impacts range from $2,038 to $194,035. The most common 95% of breach impacts range from $826 to $653,587.

TOP 5 ACTION VARIETIES IN BREACHES IN 2020:

- Phishing (up 11% YOY)
- Use of stolen credentials
- Other
- Ransomware (doubled YOY)
- Pretexting

TOP 3 DATA VARIETIES IN BREACHES:

- Credentials
- Personal
- Medical

Aggregation

If putting all your information online and in one place sounds like a good idea, there are many companies—often called data aggregators—ready to help you organize your IT environment. However, before you share your account information and other sensitive data with data aggregators, it pays to know how these services operate, and how to protect yourself from potential privacy and security risks.

At its most basic, financial data aggregation puts information about your financial holdings under one roof. Your "dashboard“, sometimes called a management hub or portal, can display your investments, savings, insurance policies, credit transactions, and other sensitive information.

EXAMPLES OF AGGREGATORS

- SolarWinds
- Blackbaud
- Microsoft 365

Insight & Experience:
Bill Bussiere

The State of Cybersecurity

- SMB companies are more likely to experience a breach
- Cybersecurity events have outsized impacts on SMBs
- Compromised or stolen credentials and cloud misconfigurations are leading vectors for a breach

- Average cost of a breach with under 500 employees is $2.64M
- Average cost of each PII record compromised is $150
- Data breach costs continue to rise

- Average number of days to identify a breach is 201 days
- The average number of days to contain a breach is 72 days

Cybercrime is up

600%

due to COVID-19 pandemic

80%

of breaches are customer PII

Potential Damages

Cybersecurity is always top of mind for everyone, but it's even more important during COVID-19, as a breach could be what closes a company's doors for good.

Don't be average:

THE AVERAGE COST OF A DATA BREACH IS

$3.86M

as of 2020

THE AVERAGE TIME TO IDENTIFY A BREACH WAS

207

days in 2020

THE AVERAGE LIFECYCLE OF A BREACH WAS

280

days from identification to containment

IBM, (2020). Cost of Data Breach Report 2020. How much would a data breach cost your business? Retrieved from https://www.ibm.com/security/data-breach

Milkovich, Devon. 2020, December 23).15 Alarming Cyber Security Facts and Stats. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/.

Lifecycle of a Data Breach

Breakout
Attackers will use their initial access to compromise other computers within 9 hours on average, sometimes as fast as 20 minutes (CrowdStrike, 2020)

9 Hours

13 Hours

Data Access
Within 4 hours after the initial compromise, an attacker has likely found your most sensitive data. (Moss Adams penetration testers' experience)

Breach
Within 16 hours of initial compromise, the attacker has copied your data to their own systems. (Moss Adams penetration testers' experience)

16 Hours

201 Days

Detection
It takes most organizations 201 days to detect that they've been breached. (Ponemon, 2020)

Containment
From the date the breach was detected, it takes another 72 days on average to contain the breach. (Ponemon, 2020)

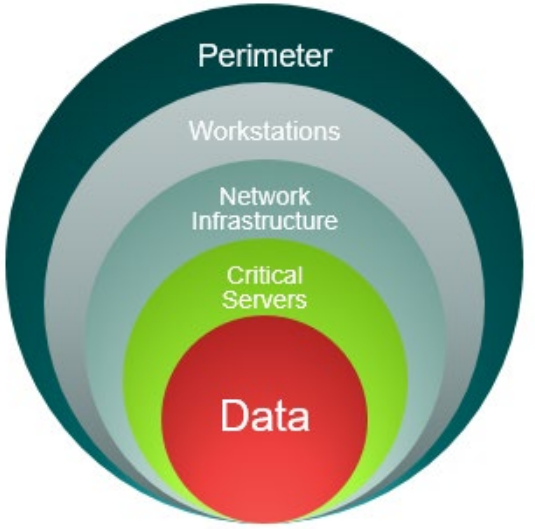
273 Days

Cyber Adversaries and Their Motivation

ADVERSARY	MOTIVE
Malicious Insider	Financial gain or grievance (typically perpetrated by disgruntled, troubled, or greedy insiders)
Inadvertent Insider	No motive (insider unknowingly falls victim to common social engineering tactics, such as phishing, vendor spoofing, or pretexting)
Hacker	Thrill of gaining access to secured systems (typically looking to prove themselves and get bragging rights)
Cybercriminal	Financial gain – novices through use of Crimeware-as-a-Service (CaaS)
Cyber Hacktivist	Promote a political agenda or social change
Cyber Terrorist	Motivated by a political, religious, or ideological cause (the goal is to intimidate government, section of the public, and/or interfere with critical infrastructure)

Defense-in-Depth

- Defense-in-depth is a layered approach to information security focused on fundamentals.
- Multiple controls are in place to defend against different types of attacks or failures such as:
  - Firewalls
  - Endpoint security
  - Regular patching
  - Policies and procedures
  - Security awareness training
  - Third-party vendors
  - Credentials and access management
  - Backup and recovery



Internal controls have to be validated to provide confidence

Infrastructure Design

1. No right or wrong
2. Determine your tolerance and criteria objectives for:
   - Availability
   - Confidentiality
   - Integrity of data
   - Integrity of processing
3. Consider technological options
4. Design infrastructure and associated controls based on these objectives:
   - Protection, detection, response
   - Encapsulation
   - Least privilege
   - Ease of access
   - Functionality
5. Consider the ROI if needed

Infrastructure Cybersecurity

TEN THINGS YOU CAN DO TO COMBAT THREATS

1. Take inventory of all your information assets and perform a risk assessment.
2. Perform hardening, such as changing the default usernames and use strong passwords on systems, network, IoT, and any key info assets.
3. Update frequently device definitions and patches on all key info assets, such as anti-virus, firewall, system software, mobile device management (MDM), and the likes.
4. Make technology choices wisely.
5. Develop a robust third-party/vendor management/review program.
6. Conduct frequent application, network, web application, and application programming interface (API) security assessments.
7. Conduct frequent security- and social-engineering awareness training.
8. Maintain appropriate cybersecurity insurance.
9. Implement real-time monitoring services (for example, firewall information networks).
10. Keep the tone at the top clear.

Cloud Design and Cybersecurity

FIVE THINGS YOU CAN DO TO COMBAT THREATS

1. Understand what the cloud provider provides: services and native security. Leverage cloud-native services/controls and automation to improve the effectiveness of security and compliance programs.
2. Build a data security strategy based on the sensitivity of the data that can meet regulations and compliance requirements as applicable to your organization.
3. Implement a least privilege architecture.
4. Secure the application “continuous integration/continuous delivery” pipeline (CI/CD), if applicable.
5. Consider other additional security/controls for your applications, devices, and networks in the cloud.

PCI Data Security Standards

PCI DSS REQUIREMENT	EXAMPLE RESPONSIBILITY ASSIGNMENT FOR MANAGEMENT OF CONTROLS		
	IaaS	PaaS	SaaS
1. Install and maintain a firewall configuration to protect cardholder data.	Shared	Shared	Provider
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	Shared	Shared	Provider
3. Protect stored cardholder data.	Shared	Shared	Provider
4. Encrypt transmission of cardholder data across open, public networks.	Customer	Shared	Provider
5. Protect all systems against malware and regularly update anti-virus software or programs.	Customer	Shared	Provider
6. Develop and maintain secure systems and applications.	Shared	Shared	Shared
7. Restrict access to cardholder data by business need to know.	Shared	Shared	Shared
8. Identify and authenticate access to system components.	Shared	Shared	Shared
9. Restrict physical access to cardholder data.	Provider	Provider	Provider
10. Track and monitor all access to network resources and cardholder data.	Shared	Shared	Provider
11. Regularly test security systems and processes.	Shared	Shared	Provider
12. Maintain a policy that addresses information security for all personnel.	Shared	Shared	Shared
PCI DSS Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	Provider	Provider	Provider

Online Security Best Practices

- Monitor online accounts
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Close or delete unused accounts
- Do not use free wi-fi
- Beware of phishing attacks
- Use anti-virus software and keep apps current
- Know how to report identity theft and cybersecurity incidents

Service Provider Security Best Practices

DUE DILIGENCE REVIEWS PRIOR TO ONBOARDING A NEW PROVIDER

- Ask them about their information security practices
  - Review policies and procedures
  - Obtain SOC 2 or SOC 1 report
  - Obtain other certification or attestations, such as HITRUST or ISO 27001
  - Ask if they have experienced a data breach
  - What type of cyber insurance do they have
- Contracts
  - Right to audit clause or require a third-party audit
  - Notification requirements for breaches
  - Compliance with records retention and destruction requirements and privacy and information security laws
  - Clear provisions on the use and sharing of information and confidentiality

Cybersecurity Best Practices

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.

Cybersecurity Best Practices (cont.)

8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any cybersecurity incidents.

POLLING QUESTION

Based on the presentation, do you foresee any cybersecurity changes for your organization?

A. No changes, we're locked down

B. We could make a few technical adjustments

C. We need to rethink our current approach, and what systems we're using

D. I'm still digesting the information

Action Items for You and Your Business

Securing information is a financial risk function. If you face a data breach, recovery costs and reputation loss can exceed estimates very quickly, so ensure you have a plan; especially because attacks will continue to evolve in sophistication. As you engage in conversations around cybersecurity and data security with your organization, consider the following best practices.

1

Educate your workforce on the threats and risks

2

Review industry best practice's cybersecurity guidance to help mitigate cybersecurity risk in your eCommerce environment

3

Hold business partners and vendors to the same standard of cybersecurity in your company

4

Manage cybersecurity risk by implementing policies and procedures, IT risk assessments, penetration testing, technical controls, security audits/reviews

E-commerce Series: Up Next

KEY TAX CONSIDERATIONS FOR YOUR E-COMMERCE COMPANY

October 28, 2021 at 10AM

QUESTIONS

Let’s start a conversation.

francis.tam@mossadams.com

The material appearing in this presentation 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, it 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.

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

THANK YOU