PROVIDENCE BUSINESS NEWS

PBN SUMMIT

CYBERSECURITY

#PBNCyberSummit

PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

GUEST MODERATOR

Doug White

Chair, Cybersecurity and Networking, Roger Williams University & Podcast Personality, Security Weekly

#PBNCyberSummit

PROVIDENCE BUSINESS NEWS

PBN SUMMIT CYBERSECURITY

PANELISTS

Jason Albuquerque
Chief Information Security Officer
Carousel Industries

Colin Coleman
Partner
Partridge Snow & Hahn

Cindy Lepore
APV, Business Insurance Marsh & McLennan Agency

Eric Shorr
President
SecureFuture Tech Solutions

Francesca Spidalieri
Senior Fellow,
Cyber Leadership
The Pell Center, Salve Regina

Jeffrey Ziplow
Cybersecurity Risk Assessment Partner
BlumShapiro

#PBNCyberSummit

Secure Future
TECH SOLUTIONS
Proactive Today for a Brighter Tomorrow

15 Ways to Protect Your Business From A CYBER ATTACK

Don't be a sitting duck to Cyber Criminals!!

15 Ways To Protect Your Business From A Cyber Attack!

Security Assessment
It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?
Date: _____

Spam Email
Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

Passwords
Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

Security Awareness
Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

Did you know?
1 in 5 Small businesses will suffer a cyber breach this year.

81% Of all breaches happen to small and medium sized businesses.

97% Of breaches could have been prevented with today's technology.

Advanced Endpoint Detection & Response
Protect your computers adata from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

Multi-Factor Authentication
Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

Computer Updates
Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

Dark Web Research
Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

SIEM/Log Management
(Security Incident & EventManagement)
Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

Web Gateway Security
Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

Mobile Device Security
Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

Firewall
Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

Encryption
Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

Backup
Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

Cyber Insurance If all else fails, protect your income and business with cyber damage and recovery insurance policies.

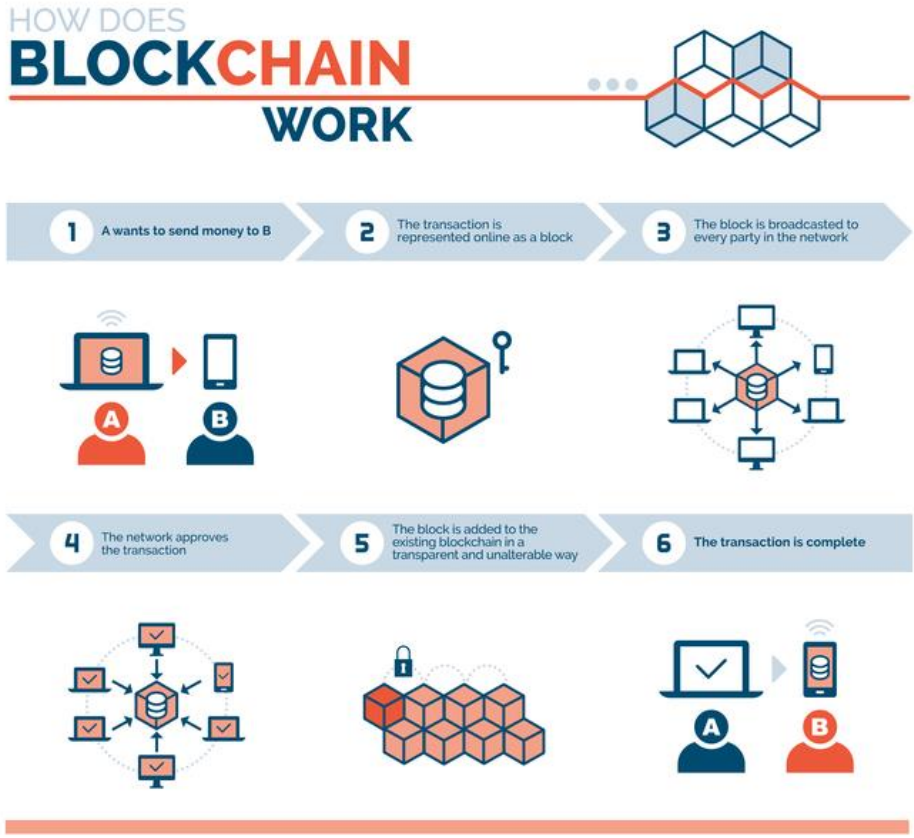
Five Functions of NIST CSF

Product Landscape

Responsibility Landscape

Cyber Resilience

Blockchain Basics



Big corporations may grab the headlines…

Equifax breach exposed data for 143 million consumers

Facebook Security Breach Exposes Accounts of 50 Million Users

YAHOO!

amazon.com and you're done.™

Former Equifax Executive Pleads Guilty to Insider Trading

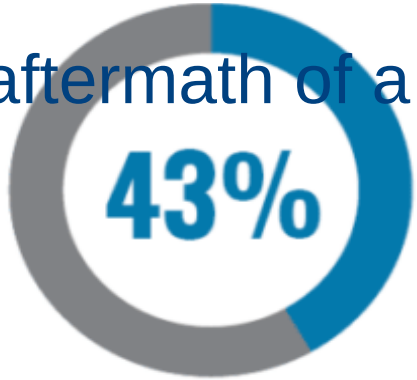
By The Associated Press

Marriott Hacking Exposes Data of Up to 500 Million Guests

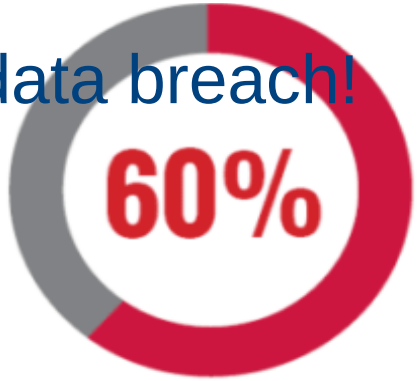
DoorDash Says Data Breach Affected 4.9 Million People

A hacker gained access to 100 million Capital One credit card applications and accounts

…But small businesses have the most to lose in the aftermath of a data breach!



of cyber attacks are targeting small businesses



of small companies go out of business within 6 months of a cyber attack

average spent because of damage or theft of IT assets

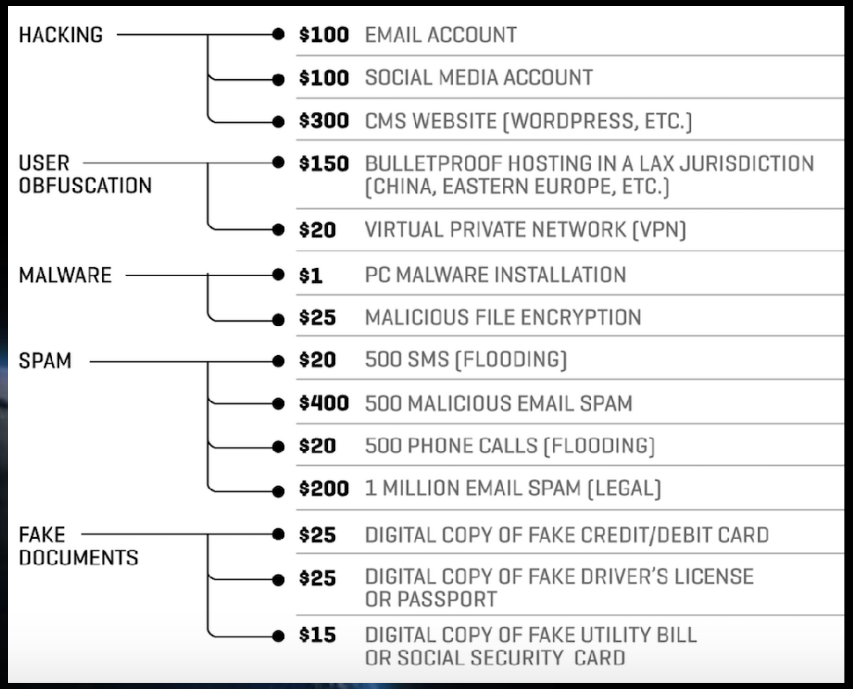
said a negligent employee or contractor was the root cause of the attack

Cyber tools are cheap, accessible, and easy to use

Personal Identifiable Data is Available

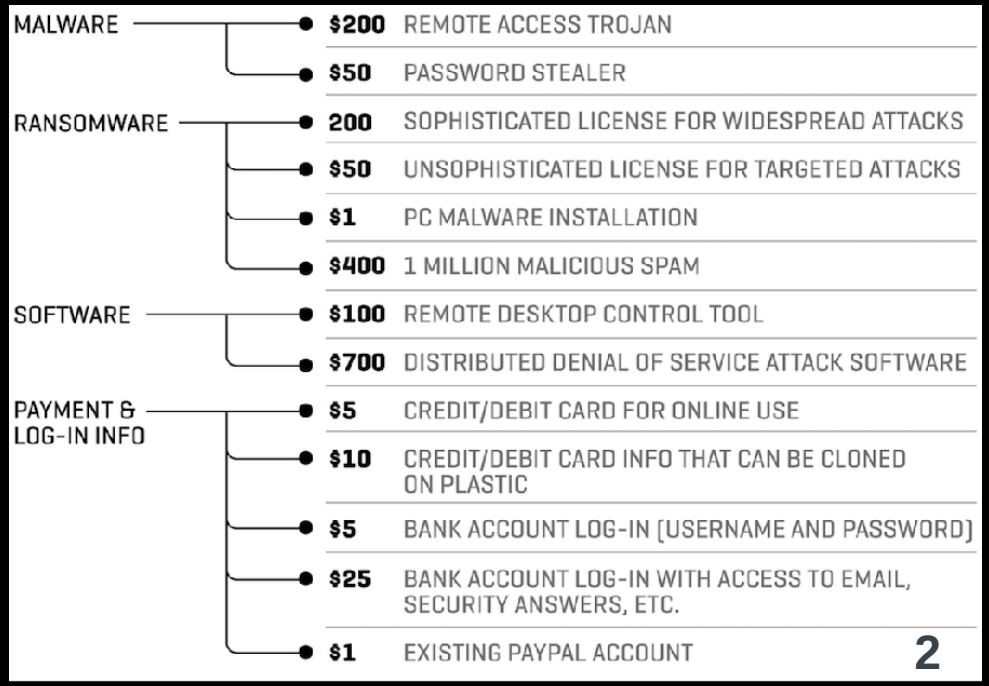
PERSONAL INFORMATION	$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
	$150	CREDIT REPORT 750+ CREDIT SCORE
DATABASE RECORDS	$25	1 MILLION COMPROMISED EMAIL/PASSWORDS

Services are Available



HACKING	$100	EMAIL ACCOUNT
	$100	SOCIAL MEDIA ACCOUNT
	$300	CMS WEBSITE (WORDPRESS, ETC.)
USER OBFUSCATION	$150	BULLETPROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
	$20	VIRTUAL PRIVATE NETWORK (VPN)
MALWARE	$1	PC MALWARE INSTALLATION
	$25	MALICIOUS FILE ENCRYPTION
SPAM	$20	500 SMS (FLOODING)
	$400	500 MALICIOUS EMAIL SPAM
	$20	500 PHONE CALLS (FLOODING)
	$200	1 MILLION EMAIL SPAM (LEGAL)
FAKE DOCUMENTS	$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
	$25	DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
	$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD

Access & Weapons are Available



MALWARE	$200	REMOTE ACCESS TROJAN
	$50	PASSWORD STEALER
RANSOMWARE	200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
	$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
	$1	PC MALWARE INSTALLATION
	$400	1 MILLION MALICIOUS SPAM
SOFTWARE	$100	REMOTE DESKTOP CONTROL TOOL
	$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
PAYMENT & LOG-IN INFO	$5	CREDIT/DEBIT CARD FOR ONLINE USE
	$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
	$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
	$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
	$1	EXISTING PAYPAL ACCOUNT

The average organization takes approximately

206 days to identify that an incident

has occurred

and 73 days to contain it.

The number one cause of cyber breaches

are a company's own employees!

Cybersecurity awareness training

Organizations are devoting more time and resources to raising awareness about **cyber threats**, investing in security measures, and training their employees about the risks of phishing, malware, and weak passwords.

1. Use two-factor authentication to log into emails, VPNs, databases, and important websites — it can prevent 99% of attempted account compromises, spam, & IP theft;
2. Use VPN when you're not in the office or at home, especially when you're somewhere with unsecured Wi-Fi or in a foreign country;
3. Don't respond to any emails asking you for your passwords or other login credentials;
4. Never give someone remote access to your device, even if they say they're calling from IT;
5. Double-check when clicking on links telling you to log into a company's system — verify that the URL really is your company's domain and that it has established a secure connection;
6. Don't open suspicious attachments that you weren't expecting to receive or that seem odd;
7. Enable full disk encryption on company's devices and make sure they lock and require a password to access after being left untouched for five minutes;
8. Backup all important data, on a cloud-back storage AND a physical, offline backup system;
9. Never pay online extortion demands — it encourages crime and you might not get your data back anyway;
10. Be aware of any urgent online message or phone call with a request to provide money, gift cards, or personal information — take the time to verify things before responding.

Training, training, training…

- Choose strong passwords:
  - Use longer passwords or passphrases;
  - Upgrade password protection to multifactor authentication – this should be the default for every business;
  - Don't leave your passwords unprotected (not in a post-it note or under your keyboard!)
- Install and enable a firewall;
- Regularly update antivirus and antispyware software;
- Regularly backup all important information;
- Prioritize fixing any detected weaknesses and install patches;
- Install and enable encryption on all your devices;
- Install and enable remote wiping and/or remote disabling of mobile devices;
- Disable and do not install or use file sharing applications;
- Use social media platforms wisely;
- If you use Gmail, be aware that Google mines all data and has access to all data transmitted through Gmail, according to its terms of service.
- Avoid using unsecured or public Wi-Fi – Starbucks should not replace the office!

Assume the Internet is insecure!

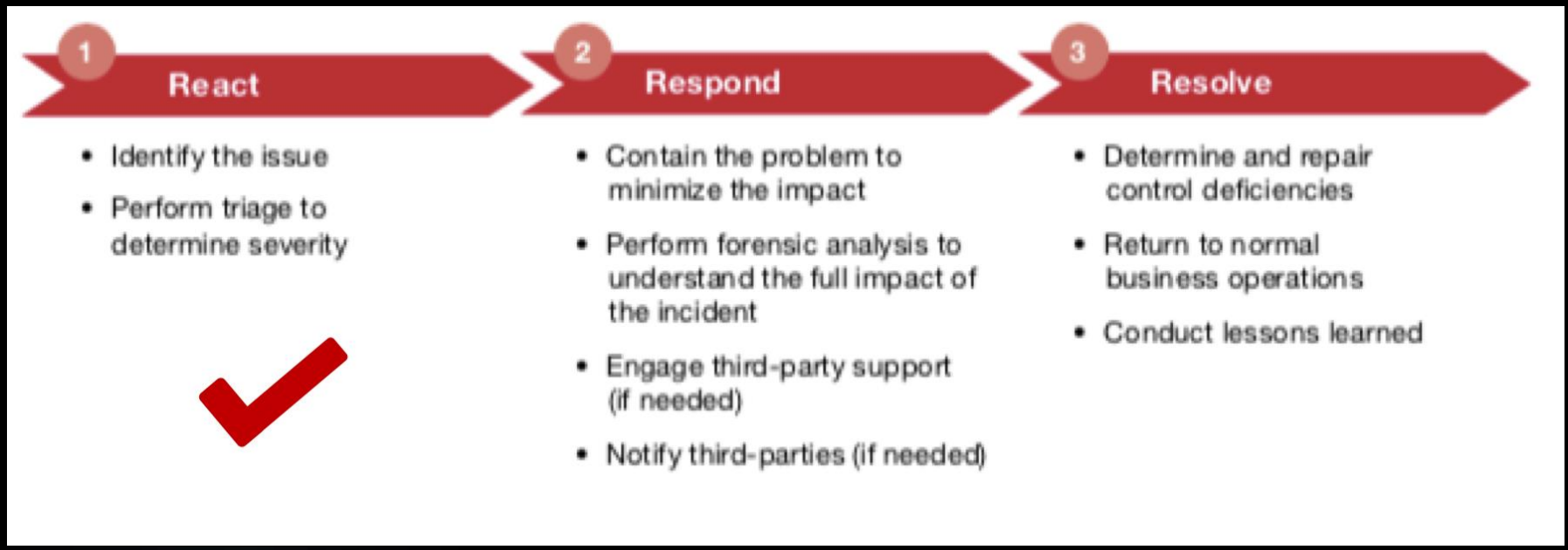
MANAGE: Develop an Incident Response Plan

- Create an Incident Response and Breach Notification Plan BEFORE an incident occurs:
  - To be effective, the incident response plan and breach notification process must be part of a comprehensive information security program:
    - Risk assessment;
    - Trigger events;
    - Mitigation plan.

- Identify national, state, and other industry-specific laws and requirements that may apply to you (e.g., HIPAA, GDPR);
- Communications/Media Team/Vendors in Place;
- Assemble an incident response team and assign overall responsibility for enterprise-wide information privacy & security oversight (appoint a data privacy and a data security officers).
- Make employees aware of the important role they play in privacy and security – your employees are your front line of defense when it comes to security (and also one of your biggest risks).

Stakeholders	• Legal • IT • Finance • Other Senior Execs
Core Team	• Incident Team Leader • Support staff • Updates to stakeholders
Investigative Team	• Technical Team Leader • Technologists or Subject Matter Experts

MANAGE: Contain, Remove, & Recover



"The greatest test lies not in the crisis itself but in the ways we respond"

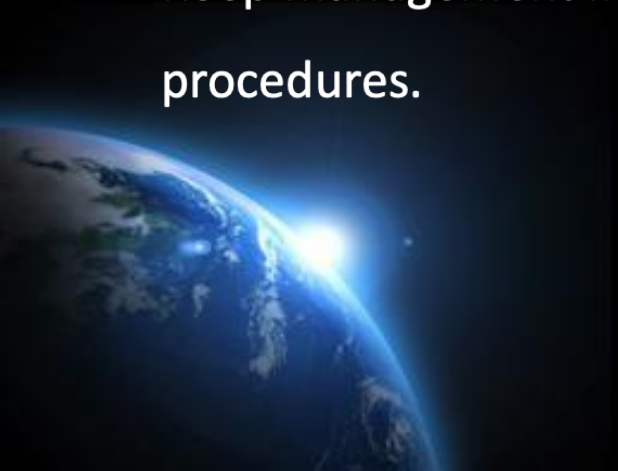
MANAGE: Determine legal implications under applicable data breaches notification laws

Under the **EU GDPR** a "personal **data breach**" is "*a **breach** of **security** leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal **data***" Art. 4(12). Organizations must notify people "*that a security incident has occurred*" within **72 hours (if feasible)** after becoming aware of the breach.

Under **U.S. state breach notification laws,** organizations must notify people if there has been a breach that exposes their ***unencrypted*** **Personally Identifiable Information (PII),** without undue delay.

MANAGE: Post-Incident Review

- Document all the steps and actions taken in response to the cyber incident – understand what actions worked well and those that did not;
- Conduct a follow-up session → discover, analyze, and review;
- Focus on improving processes and systems for the future, not assigning responsibility for the incident;
- Make recommendations for improvements & update incident response plan;
- Keep management informed and follow proper chain of command procedures.



	EU General Data Protection Regulation (GDPR)	California Consumer Privacy Act (CCPA)
Definition of Personal Information	Broad view of information "relating to an identified or identifiable natural person (**data subject**)," including individual's location, IP address, cookie identifier, RFID tags, political opinions, racial or ethnic data.	Broad view of consumers' personal information (PI). Excludes de-identified and aggregate PI and publicly available data. Exempts PI collected by a business in certain employment situations until 1 January 2021.
Jurisdiction/ Applicability	**Extraterritoriality**: Applies to all **entities** that process personal data of EU citizens, regardless of where they reside or where an entity is located. It harmonizes data protection rules across all 28 EU member states. It also regulates the transfer of personal data outside the EU.	**Extraterritoriality**: Applies to all **businesses** that collect or sell California residents' PI, whether they are located in CA or a different state/country, AND that either: 1. earn $25M/year in revenue; 2. buy or sell 50K consumer's records each year; or 3. derive 50% of their annual revenue by selling Californians' PI.
Consumer Protections/ Rights	Consumers have control over their data. They should be able to monitor, check and, if desired, delete (**right to be forgotten**) any information pertaining to them. Consent must be given in an easy-to-understand, accessible form, with a clear written purpose for the user to sign off on, and there must be an easy way for the user to reverse consent.	Consumers have control over their data. They have a right to know what data is being collected, how it is being used, and decide if it can/cannot be shared or sold, including from **data brokers** — businesses that collect and sell to third parties the PI of a consumer with whom they do not have a direct relationship.
Risk-based practices	Entities must provide a "reasonable" level of protection for personal data, including pseudonymization and encryption of protected data; appoint a data Protection Officer (DPO); conduct a Data Protection Impact Assessment (DPIA).	Businesses must implement "reasonable security measures" to safeguard Californians' PI, and include a link that says "do not sell my data" at the bottom of any page where they collect PI.
Breach Notification Requirements	Data breaches that could "result in a risk for the rights and freedoms of individuals" must be reported within **72 hours** of discovery. Data processors are required to notify consumers "without undue delay."	The California breach notification law requires entities to report a breach within **45 days**. The CCPA includes a **private right of action** against businesses that suffer data breaches.
Enforcement & Penalties	Each EU Member State designated a supervisory authority responsible for monitoring the application of GDPR within its territory. Breaches can cost up to **4% of annual global turnover or €20 million** – whichever is greater – for violation of GDPR's requirements.	Businesses that violate the CCPA will be liable for up to $7,500 for each intentional violation. Breaches can cost up to **$750/consumer/incident** or actual damages – whichever is greater – for failing to adopt reasonable data breach security practices.

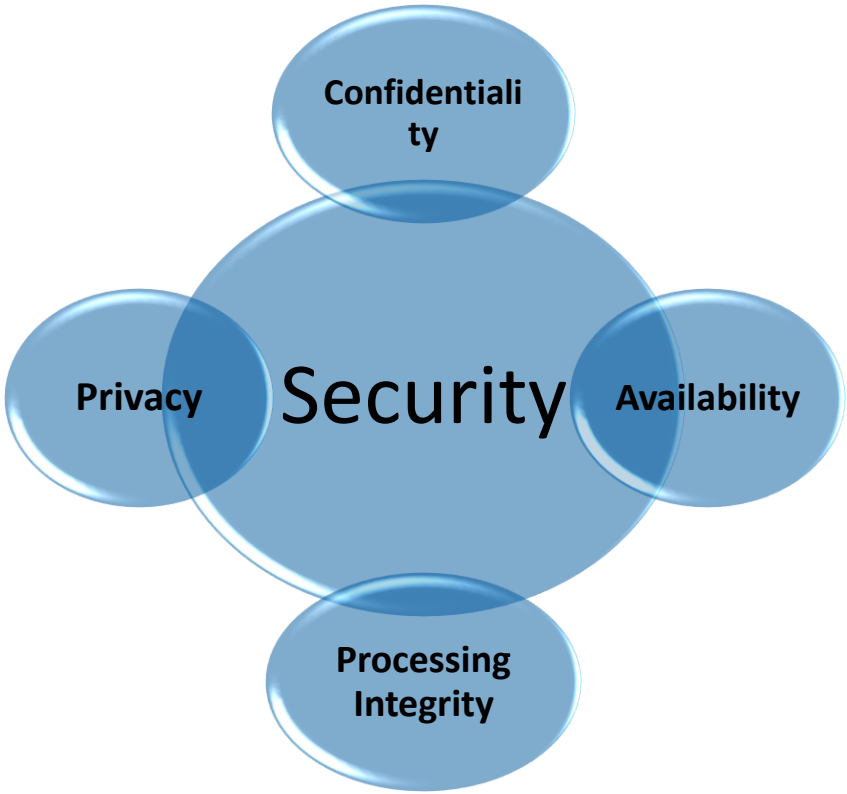
Cloud Vendors-Service Organization Controls

- Audit Report on Controls at a Service Organization.
  - Provides detailed information and assurance about the controls at the service organization.
  - Intended to meet the needs of a broad range of users
  - **SOC-1**: Internal Controls relevant to Financial Reporting
  - **SOC-2**: Security (Availability, Confidentiality, Processing Integrity, Privacy)
    - Restricted Use Reports (exception: SOC-3)
  - Type I Reports and Type II Reports

Service Organization Controls

- Type I Audit Report on Controls at a Service Organization.
  - Report on Controls Placed in Operation as of a point in time.
    - Are systems/controls fairly presented?
    - Are controls suitably designed?
- Type II Audit Report on Controls at a Service Organization.
  - Report on Controls Placed in Operation and tests of Operating Effectiveness over a period.
    - Includes testing on a sample basis.
    - Includes results of testing.

Simplifying SOC-2



blumshapiro

Simplifying SOC-2

- **Security (32 Mandatory Criteria)** – Criteria and controls to protect against unauthorized access or disclosure of information, and damage to system that could compromise the ability to meet your commitments.

  Must be included in any SOC-2 Audit.

- **Availability (+3 Criteria)** – Criteria and controls to assure the system is available for operation, use and retention.

  Think: Data Centers and SaaS providers.

- **Confidentiality (+2 Criteria)** – Criteria and controls to assure information designated as confidential or nonpublic is protected to meet your commitments.

  Think: Law Firms, Mortgage Processors, Credit Bureaus, Health / Benefit Plans.

- **Processing Integrity (+5 Criteria)** – Criteria and controls to assure that system inputs, processing and outputs are complete, valid, accurate, timely, and authorized to meet your commitments.

  Think: Payroll Providers, Data Integrators, Big Data, AI and Machine Learning

- **Privacy (+18 Criteria)** – Criteria and controls to assure that personal information, typically that which is subject to privacy regulations, is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

  Think: Healthcare or Financial Services