Breach, breach, breach…
What really matters in cyber Security?

Aka
Clarifying the fog of cyber complexity

Bottom line - As in ALL things – it is mostly about the ‘RISK value proposition!’

Using a holistic, risk-based security strategy (RBSS)
What’s Wrong With This Security?

The gates were fully locked, properly configured and validated.

I could not get through them…yet .... So use a RBSS approach!

If a capability is “invisible”, like Cyber, safety, reliability, etc, what you see is not the whole picture!
So where’s the beef (breach)?

While data breaches make the news, and there are a LOT of them, privacy fines are also ramping up globally, so what must an organization do, to show an acceptable level of cyber due diligence, especially SMBs?

While it’s partially true that there is ‘no one size fits all’ when it comes to a cyber risk posture (which tends to be 90% the same everywhere), there are some common norms to follow.

1 – Cyber security is fundamentally Enterprise Risk Management (ERM)

   What is a risk based security strategy (RBSS) and why you must have one.

2 – Do the cyber security basics well = ‘cyber hygiene’ (major elements)

3 – Know your IT/security baseline – supporting both security & privacy.

4 – Be able to show due diligence - that is - ‘reasonable’ security – yet by whose definition of what that fuzzy description entails?
“Cyber Sweet 16” Portfolio

**What is Cybersecurity** - start from the “top down” cyber view, decompose this “program” into its major elements = *Clarify the fog of cyber complexity*

- Security training, awareness, and education
- Governance, Risk & Compliance
- IoT / sensors / end points
- Cyber hygiene / CM
- Security policy
- Enterprise Access control
- Cyber safety
- Data protection & Security
- Privacy Protection
- Architecture and engineering
- Mobile & wireless security
- Compliance
- Secure SDLC (DevSecOps)
- Program management
- Threats / Intelligence Collection
- Security Monitoring & Incident Response

A huge, global sample size! This includes YOUR business too!!!

**Key Lessons Learned:**

- Hackers continue to use **known exploits**
- We have not learned from our past mistakes
- Technology alone will not stop cyber attacks

- Who is behind cyber attacks and data breaches?
  73% of cyber-attacks where caused by **outsiders**, 50% of cyber-attacks were attributed to organized crime and 12% was attributed to nation states… **motives:** 76% was attributed to financial followed by 13% to espionage which, combined, covered 90% of the incidents.

- What hacking techniques are being used?
  **Ransomware** continues to see more global use and financial impact. **DDOS** (Distributed Denial of Service) attacks, *a certain percentage of employees will always click on a hyperlink*

- What are the causes of incidents and data breaches?
  Not surprisingly, using **stolen credentials** topped the list of causes for data breaches. RAM Scrapping was high up on the list used mostly to capture more sensitive data and privileges. **Privilege Abuse** is still a major problem for organizations who fail to implement privileged access management solutions. Other common causes are **phishing** and **errors likely occurring from misconfigurations**. 28% of Incidents and Data Breaches being attributed to **insiders**, 28%

Email Continues To Be The Primary Delivery Method Of Malicious Malware (90+%)

We have met the cyber enemy, and they are **US(ers)**
2019 Security trends

With the cost of the average data breach now around the $7.8 million mark (USA), it’s essential to take cybersecurity seriously:

1. Sandbox Evaders
Newer strains of malware can now tell when they’re inside a sandbox and will respond accordingly.

2. IoT Ransomware
It costs a lot of time and money to create ransomware, so spending it on an IoT device might seem like a waste. There’s a lot of potential damage that could be caused by hackers who decide to target power grids or communications devices.

3. GDPR Compliance Lagging
Many companies might choose not to comply, erring on their ability to pay the fees for non-compliance, which they think will be cheaper than paying to comply.

4. Multifactor Authentication
Currently, the industry standard for security relies on two-factor authentication when users choose to log into the software. Most data breaches are caused by leveraging bad passwords. Since more people than ever are worried about stolen identities, we should see this kind of authentication process take off in coming years.

5. More Sophisticated Security Technology
Security is no longer solely in the hands of your IT staff. More technology is now being committed to finding out about and responding to unusual behaviors.

6. State-Sponsored Attacks
Politically motivated hackers might not just want your money. They might want access to privileged information or technology. We must also look out for our utilities, power grid and any technology that’s deployed by the military.

Pick your favorite (worst) threat – account for it in your RBSS!
Cyber Security is all about tradeoffs

Productivity  Security

Let’s build it
Cash out the benefits
Next generation can secure it

Let’s buy it, not build it
It needs ultimate security even at the cost of performance
Let’s not sell unsecure solutions

There is a middle ground
We don’t know how to consistently and predictably find it

---

With so many threats, how do try to manage them all... use a risk based security strategy, based on consequences of gaps in your cyber suite posture.

---With over 10,000 new vulnerabilities discovered this year, how can we begin to mitigate (patch) them all... use a risk based security strategy, that prioritizes vulnerabilities based on maximal risk reduction.

---Over 85% of security incidents can be minimized with effective “cyber hygiene” - doing the basics well. What are the highest risk reduction impacts therein? Using a risk based security strategy can help develop your minimized risk posture game plan.
Clarifying what really matters in Cyber Risk?

WHY - Protect the company - Optimizing resources to effectively protect and enable the business success factors, producing a best “risk value”

WHAT – Data is a company's greatest asset - thus we must provide a ‘due care’ level data assurance and provenance – using a data centric protection approach, focused on data breach risk minimization.

WHEN / WHERE – Continuously / everywhere - using an adaptive risk monitoring and assessment approach, supporting the high impact risk mitigations that offer the best company success factors utility and value.

HOW - Taking an overall, enterprise, holistic security approach, using a risk based security strategy (RBSS) to capture and resource best risk values.

Cyber Security always costs too much, until it’s not enough (data breach).

Hindsight can be 20 / 20 – breaches costs avg. $4-7.8M/company
WHY manage RISK

- By being a trustworthy organization known for ‘walking the walk’ - focusing on the P&L benefits of mitigating company risks.
- Increase integrity, safety, reliability & TRUST.
- Improve our industry position, our BRAND.
- Improve resiliency (minimize down time, lost efforts)
- Improve compliance levels, enhance efficiencies.

- DATA rules in every industry– security counts as does privacy – thus show excellence therein. **ANY data breach could cause loss of business**
- Improving processes and supporting new services and products (enhance business groups productivity) = **increased customer experience = revenues**.

---

**Integrate a Holistic RBSS into our Company ERM Effort**

- Enhance, streamline current security based efforts
- Increase risk awareness and support in the company
ASSUME a BREACH – then prepare for it

Some FUD to start with (e.g., Fear, Uncertainty and Doubt)

2018 - SIX Third-Party Breach Examples (of many) (as was TARGET!)

- TCM Bank – cause was a misconfigured website managed by a third-party
- Lifelock, cause was with a third party, managing the opt-out marketing page
- Ticketmaster, caused by maliciously manipulated code that was created by Inbenta Technologies (third party).
- GM, Fiat Chrysler, Ford, Tesla, Toyota, and Volkswagon, caused by a vendor / 3rd party (Level One Robotics), by using a poorly protected data transfer protocol.
- Nuance, a third-party provider of speech recognition software, exposed 45,000 patient records … caused by a former Nuance employee had hacked into the company’s servers and accessed the patient information.
- [24]7.ai, provider of online chat and support services —including Sears, Delta Airlines, and Best Buy. They did not disclose the cause, but likely third party based, whereas estimates are between 60% and 70% of all breaches currently result from third-party security failures

Use a holistic RBSS to manage priorities and resources

https://www.darkreading.com/attacks-breaches/6-eye-raising-third-party-breaches/d/d-id/1332522
ASSUME a BREACH – then prepare for it

Preparations – what to do before the breach - mitigate the high threat vectors! 
(using the NIST CSF – identify, protect and detect)

• **Users** – cyber education (anti-phishing training), “NextGen AV”, and URL filtering
• **Data exfiltration** – encryption, data leak prevention (DLP), access controls (IAM & RMS)
• **Ransomware / crypto mining** – secure backup, cyber hygiene, access controls
• **Hostile intruders** – access controls, “EDR” (security tools, SIEM, MSP/MDR, etc), “CTI”
• **Mobile and “IoT”** – secure network connections, MDM, Firewall, targeted monitoring
• **Weakly managed baseline** – effective vulnerability management (patching) = CIS CSC 1-8
• **3rd Party risk management** – Assessment policy / survey, updated contracts, monitoring

After the event, *(NIST CSF respond and recover)*

**Practiced computer response plan**

– clear immediate actions, roles and responsibilities, especially stopping the attack, limiting damage, communicating the situation – be careful of what is disclosed to whom (loose lips).

- **Handling a potential data breach is crucial** – BE SURE it is one, as the clock starts once assessed as to notification time frames *(BTW, all 50 states exempt this IF using encryption)*.

Use a holistic RBSS to manage priorities and resources
So what’s an organization to **DO?**
*(example ‘best practices’ from **NIST**)*

Small Business Information Security: The Fundamentals *(**NISTIR 7621 R1**)*

- Uses same **NIST CSF five functions** – **Identify**, **Protect**, **Detect**, **Respond** and **Recover**.
- **Identity** - Control access, create information security policies, conduct risk assessment.
- **Protect** - patch systems, use firewalls, secure wireless, use email security, use encryption, train users.
- **Detect** - anti-virus / malware programs, monitor activity and logs (SIEM, system parameters, etc), other “IoC’ detection security tools.
- **Respond** – Incident response plan and disaster recovery – stop the attacks, limit damage.
- **Recover** – full, secure backups, consider cyber insurance, continuous process and technology improvements.
- Also, “**work safely**” – use anti-phishing email practices, situational awareness, do not connect unauthorized devices to network nor download software from unproven sites, be aware of social engineering tactics, etc.

**Use a holistic RBSS to manage priorities and resources**

Risk mitigations / types

Risk management = avoid, reduce, accept, or transfer
(And exploit and ignore)

Proving a due diligence level of security
Foundation to minimizing risk and legal liability

Data breaches = 1st & 3rd party liability, the latter can be global, almost unbounded!

Cyber risks are pervasive – are you covered?

For example, Cyber Insurance is a Transfer of Risk
A risk-based approach means that asset owners and operators identify, assess and understand the cybersecurity risks to which they are exposed, and take protective measures commensurate to those risks in order to mitigate them effectively.

- Understanding and prioritization RISKS are key activities

The risk assessment therefore provides the basis for the prioritized application of cyber-protective actions and measures.

Overall RBSS approach:

- Threat Modeling of the potential avenues for attack.
- Identify solutions and methods for the detection and defense.
- Develop a framework to address a defensive approach while understanding the impact to the business.

The RBSS approach is not a “zero failure” method; there may be occasions where an institution has taken all reasonable measures to identify and mitigate cybersecurity risks, but it still suffers successful attack.
So what’s a “RBSS”?

*How to develop and enable a RBSS approach.*

Construct your most likely threat vectors – which align with your organization, standard TTPs and where / how they act in the ‘cyber kill chain’ model. These are your ‘use cases’ to apply to the mitigations.

Do the security basics well – cyber hygiene (e.g., the CIS CSC 1 – 8) (statistically this will reduce security incidents by over 80-85%)

Use your risk assessment – as part of an integrated Enterprise Risk Management (ERM) Plan – map the gap mitigations (priorities & resources) (various tools: risk register, risk ‘heat map’, map to business outcomes)

Cyber Threat Intel - keep abreast of the new threats, attacks in progress (monitor several sources for CTI, integrate into vulnerability management)

Use a holistic RBSS to manage priorities and resources

*We can share the RBSS plan we use!*
RBSS mitigation “effects”

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence / Severity</th>
<th>Strategic Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Very High</td>
<td>A. Market Share - <em>Growth</em> - Any data breach (disclosed) will cause a loss in clients and minimize new ones</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>B. Customer trust &amp; relationship - <em>Delighted fan</em> - Similar to #1, we lose their confidence; thus trust in our work, brand</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>C. New business; - <em>New markets</em> - Similar to #1, potential clients will take their business elsewhere</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>D. Global presence - <em>International market + GDPR</em>. Unable to be certified, or prove we are privacy stewards…</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>E. Regulatory compliance - <em>Stay ahead of tax changes / compliance</em>. Increased litigation, costly fines, penalties, etc</td>
</tr>
</tbody>
</table>

How the mitigations capabilities can affect the risk reduction levels
Typically reducing likelihood (threats) and / or consequence (Impact)
Cyber Hygiene

What, Why & How
Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.
Common Hygiene problems

- **Loss of Data**: Hard drives and online cloud storage that isn’t backed up or maintained is vulnerable to hacking, corruption, and other problems that could result in the loss of information.
- **Misplaced Data**: Poor cyber hygiene could mean losing data in other ways. The information may not be corrupted or gone for good, but with so many places to store data, misplacing files is becoming increasingly commonplace in the modern enterprise.
- **Security Breach**: There are constant and immediate threats to all enterprise data. Phishing, hackers, malware, spam, viruses, and a variety of other threats exist in the modern threat landscape, which is constantly in a state of flux.
- **Out of Date Software**: Software applications should be updated regularly, ensuring that the latest security patches and most current versions are in use across the enterprise – for all applications. Out of date software is more vulnerable to attacks and malware.
- **Older Security Software**: Antivirus software and other security software must be updated continuously to keep pace with the ever-changing threat landscape. Outdated security software – even software that has gone a few months without an update – can’t protect the enterprise against the latest threats.
RBSS - CIS CSC “top 20 security controls”
Risk weighted top down - “Cyber hygiene” = 1 – 6, then add 7 & 8

IT & SEC must closely collaborate!
Hygiene Policy

ONE cyber hygiene policy version consists of these prioritized efforts:

---**One** are CIS CSCs 1, 2 & 3. HW & SW Inventory (ITAM) and Continuous Vulnerability Assessment and Remediation (patching). Within that, vulnerability priorities are (1) critical, (2) high (with a large number of occurrences), and (3) any that are “exploited in the wild.”

---**Two** is CIS CSC #4 - Control Administrative Privileges & Mgmt (PAM)

---**Three** is to **protect and recover data** (e.g., encryption, access controls, DLP/RMS, backup, etc)

---**Four** is an **effective SETA program** (security educational and training awareness), principally for anti-phishing and related technical controls (NGAV, email security, URL blocking, etc)

---**Five** is a **well-practiced CSIR Plan** (computer security incident response)

---**Six** are CIS CSCs 5, & 6. Secure Configurations for Hardware and Software and Maintenance, Monitoring, and Analysis of Audit Logs

---**Seven** are CIS CSCs 7 & 8. Email and Web Browser Protections and effective Malware Defenses

---**Eight** – **Frequent / periodic assessment** of the status and residual risks of this policy.
Hygiene resources

A - Basic Cyber Hygiene Practices That Go a Long Way
https://www.csoonline.com/article/3310068/basic-cyber-hygiene-practices-that-go-a-long-way.html

B---US-CERT SEI CERT 11 hygiene practice areas
https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf

C---A Cyber Hygiene article by alliantgroup and the National Systems Contractors Association.
http://www.industryweek.com/cybersecurity/cybersecurity-hygiene-17-steps-your-business-should-be-taking-now

D - A guide to the latest thinking around cybersecurity layering.
https://www.crainscleveland.com/guest-blogger/understanding-7-pillars-cyber-hygiene

E – A 12-Step Program to cyber hygiene
https://www.cybersheath.com/the-12-step-program-for-impeccable-cyber-hygiene/

F – 14 Ways to Achieve Basic ‘Cyber Hygiene’
https://www.nsca.org/14-ways-to-achieve-basic-cyber-hygiene/
Minimum IT Security Baseline

Threats, technical controls, & security Suite

Cyber Risk, What Really Matters?

http://www.siia.net/blog/index/Post/76999

Short answer; use a Risk Based Security Strategy (RBSS). One that focuses on cyber hygiene, access management, encryption and monitoring (along with an effective third party/vendor risk management effort)
Minimum IT/Security baseline

First Select YOUR Current Threat / Risk vectors

- **Data protection / breach** – huge negative risk consequences = $Ms at stake.
- **Phishing** – Around 95% of all security incidents start here (someone will always ‘click!’) – *therefore the technical controls must catch them* (NGAV, email security, etc).
- **Poor cyber hygiene** – known vulnerabilities not patched (97% of exploits use them).
- **Ineffective IAM / access control** – identity the new perimeter (**MFA everywhere**!).
- **Hostile intruders** – hackers, **insider threats**, careless users, any malicious user.
- **Crime as a service** (e.g., anyone can be a hacker, just pay the criminals).
- **Internet of Things / supply chain** (atypical computing devices connected).
- **Third party / vendor risks** – major threat all by itself (1/2 of breaches).
- **Regulation / compliance** (e.g., in EU GDPR, CA CCPA, FTC) – fines, loss of integrity / trust / reputation, loss of clients, competitiveness, revenue., etc

These vectors provide **your security / risk requirements**
Minimum Security Baseline
Key Technologies for GDPR Success (e.g., both data security and privacy)

Top most challenging requirements:
• Data Encryption / Pseudonymization (55%)
• Data Breach Notification Within 72 Hours (53%)
• Data Protection By Design And Default (50%)
• Data Portability (50%)
• Defining “State Of The Art” (47%)

Top most challenging compliance actions:
• Understand Areas Affected And Requirements (59%)
• Data Classification (54%)
• Data Loss Prevention ((53%)
• Employee Education (51%)
• Anonymize Privacy Data (50%)

ALL the GDPR requirements require an underlying technical controls basis.

Technical Controls - Compliance Methods

• **Change management**: Monitors, logs, and reports on data structure changes. Shows compliance auditors that changes to the database can be traced to accepted change tickets.

• **Data discovery and classification**: Discovers and provides visibility into the location, volume, and context of data on premises, in the cloud, and in legacy databases. Classifies the discovered data according to its personal information data type (credit card number, email address, medical records, etc.) and its security risk level.

• **Data loss prevention**: Monitors and protects data in motion on networks, at rest in data storage, or in use on endpoint devices. Blocks attacks, privilege abuse, unauthorized access, malicious web requests, and unusual activity to prevent data theft.

• **Data masking**: Anonymizes data via encryption/hashing, generalization, perturbation, etc. Pseudonymizes data by replacing sensitive data with realistic fictional data that maintains operational and statistical accuracy.

• **Data protection**: Ensures data integrity and confidentiality through change control reconciliation, data-across-borders controls, query whitelisting, etc.
Technical Controls - Compliance Methods

- **Ethical walls**: Maintains strict separation between business groups to comply with M&A requirements, government clearance, etc.

- **Privileged user monitoring**: Monitors privileged user database access and activities. Blocks access or activity, if necessary.

- **Secure audit trail archiving**: Secures the audit trail from tampering, modification, or deletion, and provides forensic visibility.

- **Sensitive data access auditing**: Monitors access to and changes of data protected by law, compliance regulations, and contractual agreements. Triggers alarms for unauthorized access or changes. Creates an audit trail for forensics.

- **User rights management**: Identifies excessive, inappropriate, and unused privileges.

- **User tracking**: Maps the web application end user to the shared application/database user to the final data accessed.

- **VIP data privacy**: Maintains strict access control on highly sensitive data, including data stored in multi-tier enterprise applications such as SAP and PeopleSoft
Minimum technical measures

• **Firewalls** which are properly configured and using the latest software and key security features.

• **User access control management** by, for example, the UAC functionality in Windows. In order to comply with the law, there should be no one person in your organization with full access to all files and even your network administrator should have restricted access.

• **Unique passwords** of sufficient complexity and periodic expiration on all devices (including mobile phones) to defend against dictionary and rainbow table attacks. *Consider MFA everywhere*, especially for remote access.

• Timely decommissioning and **secure wiping** (that renders data unrecoverable – “NSA” approved) of old software and hardware

• **Incident / breach response plan**, processes and messaging.
Minimum technical measures

- Real-time protection anti-virus, anti-malware and anti-spyware software
- Encryption of all portable devices ensuring appropriate protection of the key
- Encryption of personal data in transit by using suitable encryption solutions. This may include SSL and IPsec VPN connections which are appropriate for machine-to-machine connections.
- Intrusion detection and prevention systems
- Secure data controls (DLP/DRM) in the cloud and backup
- Monitoring and audit capabilities, preferably continuous
- Secure configuration on all devices (including mobile phones)
- Regular software updates, using patch management software
Security architecture / roadmap

Big picture GOAL
What is “reasonable security”?

And WHO says so?

https://www.rgcybersecurity.com/cybersecurity-risk-reasonable-posture/
Cybersecurity Risk, what does a “reasonable” posture entail and who says so?

With data breaches seeming to permeate the headlines daily, and hackers developing innovative methods to penetrate cyber defenses, businesses must contemplate what “reasonable” security posture it must implement for WHEN, not IF, a data breach occurs. Then determine how that translates into an adequate due diligence level of security within the confines of our organizational responsibility of due care to manage enterprise risks effectively?

Virtually all references to ‘reasonable security’ are high level and vague; whereas the source can’t possibly know the many environments that exist. Instead, only generalizations and risk-based truisms act as guides. Additionally, the cyber risk lexicon differs depending on industry and audience (and then having to decide which framework to follow (NIST, COBIT, ISO, etc)).

Thus it’s no surprise authoritative entities don’t want to box themselves in with a specific definition of what constitutes as “reasonable” security, as once that happens resources would be required to support that position and defending the many nuances that follow in court cases. Alas, the status quo of vagueness and open to interpretation continues (aka, the proverbial and frustrating “it depends” response).

(Excerpts from the article)
Cybersecurity Risk, what does a “reasonable” posture entail and who says so?

Part of the underlying problem with establishing a set cybersecurity duty of care is due to the **ever-changing cyber threat landscape and the fact that each data breach is unique**. Accordingly, litigation arising from data breaches can be brought in various forms of action. Whether a suit is brought from a regulatory agency such as the Federal Trade Commission or the Securities Exchange Commission, shareholders or a group of individuals, **courts engage in some form of analysis of whether or not a company breached some type of duty or failed to apply a reasonable standard of care in protecting sensitive information**.

In terms of establishing a standard of care in the tort of negligence, the word “reasonable” is somewhat a term of art that has evolved in response to advances in technology. A defendant must show that its actions conformed to a standard of conduct equivalent to that of another that would be considered “reasonable … under like circumstances” to avoid liability for negligence. **Courts commonly use a “risk/utility” test to analyze whether a defendant’s conduct conformed to others similarly situated in the same industry and if the potential harm outweighs the burden of implementing the proper measures to prevent such harm**. At its core, the risk/utility formula seeks to determine if the burden of placing adequate precautions in place is less than the potential risk of injury and the gravity of the injury. *(aka, plaintiffs must also prove HARM)*
Cybersecurity Risk, what does a “reasonable” posture entail and who says so?

Given the absence of an exact definition of what “reasonable” security practices entails, a simpler approach is to instead, evaluate what constitutes a lack of reasonable security. This approach makes it easier for an organization to map their data security protection efforts (including privacy and resources) to a known framework and more effectively quantify the residual risks – the end state that is most useful and uses common risk terminology. By using the Center for Information Security (CIS) Critical Security Controls (CSC) as the overall cyber risk authoritative source, one just needs to map any reasonable definition to those 20 specifications to attest to its validity and utility.

Why did we choose CIS CSC approach for reasonableness versus others, for example the NIST Cybersecurity Framework (CSF) or others (such as COBIT, ISO27001, HITRUST, etc)? As major privacy laws are enacted, such as the EU’s GDPR, and CA’s CCPA, the residual risk definition and determination has become even broader, covering many more requirements. This translates to what is a reasonable security posture, upon which privacy environments are typically built. Our proposed method to quantify what is reasonable (or is not, as in this case), is using the CA definition provided in early 2016 by the Attorney General. While the definition does not apply directly to states outside of CA, the recent CCPA will apply and the CA AG “reasonable” definition will likely be invoked in most CA privacy court cases.
Cybersecurity Risk, what does a “reasonable” posture entail and who says so?

The Report Recommendation states that, ““The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security” (pursuant to California’s information security law).”

California’s information security statute, Cal. Civ. Code § 1798.81.5(b), requires that: “[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

CIS CSC is 20 cybersecurity control measures meant to “detect, prevent, respond to, and mitigate damage from cyber attacks. https://learn.cisecurity.org/cis-ram-download

While the CA AG’s formal position is not codified in law and therefore not binding, this definition of “reasonable security” does appear to strongly suggest that failure to implement all of the CIS CSC that apply to an organization constitutes a lack of reasonable security.” There is little (if any) downside to using the CIS CSC - period - as those security controls are definitive and actionable from the start, providing a foundational risk posture. That view will support any conflict resolution venue (arbitration, courts, etc) and further the organization’s risk management savvy and expertise (both in source chosen (NIST, COBIT, etc) and integrating into an ERM).
RECAP – what really matters?

1 – Cyber security is fundamentally **Enterprise Risk Management (ERM)**
   Use a risk based security strategy (**RBSS**) and prioritized mitigations.

2 – Do the cyber security basics well = ‘**cyber hygiene**’
   (enforced through policy)

3 – Know your **IT/security baseline** – supporting both security **and** privacy.

4 – Be able to show due diligence - that is - ‘reasonable’
   security – **assess risk using the CIS CSC**

Pick a framework, implement an ERM, use a RBSS based on CIS CSC
**SHOWs dues diligence = sleep at night!**

Mike.Davis.SD@gmail.com
Background
..Errata..
RISK resources

Risk Management Framework for Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Cybersecurity for Small Business (many links to resources / references)
https://www.fcc.gov/general/cybersecurity-small-business

Risk Management for Small business

CIS RAM (Center for Internet Security® Risk Assessment Method)
An information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls™ cybersecurity best practices.

the DHS CRR - may be the best path?
https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

IT risk assessment frameworks: real-world experience

The Security Risk Assessment Tool (SRAT)
a free resource for both experienced security managers and those new to risk assessments.
RISK resources

Cyber Risk Management Resources (numerous links!)

Security Risk Assessment Tool (SRA Tool)
Version 3.0.1 of SRA (78MB)
https://www.healthit.gov/sites/default/files/SRA-Tool-3.0.1.msi

How to Perform IT Risk Assessment (“101”)
RA checklist
https://www.netwrix.com/landing/downloaddoc?key=4eb49bc1ece4222fc3db49dd80afc67b9411d53a64169cbb12724dd57243c686

Risk Appetite Statements
https://www.theirm.org/media/3296897/0926-IRM-Risk-Appetite-12-10-17-v2.pdf

AND MORE…
https://www.nist.gov/cyberframework/small-and-medium-business-resources
https://www.nist.gov/itl/smallbusinesscyber
https://www.us-cert.gov/resources/smb
**Username & Passwords**
Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:
- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.
- Your UPS or FedEx accounts, where they ship stolen goods in your name.

**Email Harvesting**
Once hacked, cyber criminals can read your email for information they can sell to others, such as:
- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

**Virtual Goods**
Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:
- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

**Botnet**
Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:
- Sending out spam to millions of people.
- Launching Denial of Service attacks.

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

**Identity Hijacking**
Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:
- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

**Web Server**
Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:
- Hosting phishing websites to steal other people's usernames and passwords.
- Hosting attacking tools that will hack people's computers.
- Distributing child pornography, pirated videos or stolen music.

**Financial**
Once hacked, cyber criminals can scan your system looking for valuable information, such as:
- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

**Extortion**
Once hacked, cyber criminals can take over your computer and demand money. They do this by:
- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

www.securingthehuman.org/ouch

Too small to read, just know the types

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com
RECAP, so what DOES matter in Cyber?

CYBER is fundamentally all about **TRUST** and **DATA**

(Identity, authentication, secure comms -- assurance, encryption, data controls, quality)

It’s NOT about chasing new cyber capabilities / “silver bullets”
Rather doing the fundamentals well, prioritizing and acting on key risks and threats

85+% of security incidents are from lack of doing the basics!
With enforced: cyber hygiene, enterprise access control, & monitoring (SIEM / UEBA)
Shift from only protecting the network, to the **DATA security** itself – information centric view

Embrace your **RBSS** – *iterate and continue to reduce risk*!
Support that with an **enforceable security policy** – what is allowed / not – train to it

An **RBSS** can quantify what matters to your organization,
(as your cyber risk posture mileage will vary (it depends))
just ensure you capture and communicate it well.
Business Objectives & Success Factors.

Using a notional set of Strategic Goals as a guide, we propose five business success factors to assess RBSS mitigations and the key risks / impacts therein.

A - **Market share** – *Growth* - Any data breach can cause a loss in clients and minimize new business opportunities

B - **Customer trust & relationship** - *Delighted fan* – Added to #1, we lose their confidence; thus trust in our work, brand

C – **New business** - *New markets* - added to #1 & 2, potential clients will take their business elsewhere

D – **Global presence** - *International market + GDPR*. Unable to be certified, or prove we are privacy stewards… reduce our opportunities..

E - **Regulatory compliance** - must demonstrate due care; Stay ahead of tax changes / compliance. Avoid increased litigation, costly fines, penalties, etc

ALL of these success factors can *be significantly, negatively affected* by:

1. *Data breach (ineffective data assurance)*,
2. *Fines and bad PR for non compliance (and soon GDPR)*, and
3. *Inadequate IT/Security capabilities.*
Yes, “RISK” really is ALL about the DATA*

“Future” Data Vision

Themes and Memes (Technology vs Technology Adoption)

Convergence = Genomics, Robotics, Informatics, Nanotech (each a $B+ market)

“CBAD” = Cloud, Big Data, Analytics, Data Science (are you ‘all in?”)

Telematics = Sensing robotics, Cyber Physical Systems (will kids need to learn to drive?)

Interactive 3D = Augmented Reality, HTML 5, Three.js (3D graphics for WebGL)

Embedded Computing = eHPC, Tessel (mcu / java), Programmable hardware

LBS = Location Based Services, IPS, Beaconing, NFC

IoT = Internet of Things, M2M, Connected cars, Quantified Self

Mobilization = Preparation for Conflict/Competition, Autonomy, The Draft

STEM = Science Technology Engineering Math , Generation NOW, Old Dogs (YOU)

Infinite sources

Unstructured data = 80%

Data Security and Compliance

The Landscape

Protect data and privacy: at rest, when processing AND in transit.

* and trust / assurance!
RISK “101” -two main factors – **likelihood and Impact** – BOTH must be managed

**Likelihood** – threats x vulnerabilities – minimize both, numerous vectors / mitigations

**Impact** – loss of resource / business capabilities – data security & privacy protection

**Risk mitigation methods:**
- **Ignore** – assume it won’t happen
- **Avoid** – change processes, connections
- **Transfer** – cyber insurance, 3rd party assume
- **Mitigate** – implement capabilities and reduce:
  - threats – security tools, SIEM, MDR, etc
  - vulnerabilities – patching, policies, etc.
  - possible impacts – data security & privacy protection

2019 security focus changing from **likelihood** to **impact reduction**

Major business risks: loss of confidence and trust and ability to do business globally
The risk “heat map” is a common way to report and visualize risk.
**RBSS – Risk Management** -- Risks Minimized Within Risk Tolerance

Major **business risks**: loss of confidence & trust, and ability to conduct business

Major **causes**: data breach, threat minimization and compliance

<table>
<thead>
<tr>
<th>Business Impact</th>
<th>Likelihood of Incident Scenario</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Probably</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R1</td>
</tr>
<tr>
<td>Large</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R2</td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R3</td>
</tr>
<tr>
<td>Small</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Insignificant</td>
</tr>
<tr>
<td>Insignificant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend**

- **Current Risk**
- **Target Risk**

**Risk**
- R1: Loss of confidence and trust (e.g., *data breach risk*)
- R2: Loss of confidence and trust (e.g., *KEY threat minimization*)
- R3: Ability to do business globally in a regulated market (*compliance*)

**Organization Risk Tolerance**

- Must define / agree to this level
- Quantify the “risk appetite”
- Use risk register to formally accept risk

For maximal company protection coverage, the **residual cyber risks** must be integrated into an overall company Enterprise Risk Management (*ERM*) Program.
Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines implementing and operating the systems supporting the organization’s core missions and processes.

Risk Management Frameworks (RMF) can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 2-1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (i) the organization level; (ii) the mission and business process level; and (iii) the information system level.

- Embrace the ERM journey – *just do IT*, avoid “complexity & analysis paralysis”
- Use “A” RMF as the starting point that is aware of and responsive to the multi-stakeholder risk environment
- Tailor RMF to reflect your needs of the organization and partner / client collaboration
The Integrated **Business RM Approach**  
*Making the Risk Management Plan (RMP) work!*  

**Company Vision**  
(business success factors)

**Security Policy**  
(mobile, social media, etc)

**C&A / V&V**  
(effective / automated)

**Known Baseline**  
(assess security architecture)

**CMMI / Sustainment**  
(SoPs / processes)

**Insider Threat**  
Company Threat Intel  
(OSINT, behaviors, etc)

**Privacy by Design**  
(manage PII, HIPAA, compliance)

**SMSS / vCISO**  
(3rd party IV&V support)

**Data Centric Security**  
(DLP, reputation based methods)

**SCM / SIEM**  
(monitor / track / mitigate)

**Cyber insurance**  
(broker & legal council)

**Education / Training**  
(targeted, JIT, needs based)

**Common Business RMP model**  
(re: RMF / COBIT & Risk IT)

AND using the **NIST Cybersecurity Framework**  
(re: CAR / ESA)
RBSS Major Steps

1 – Establish a RBSS project (pick a RMF, draft a charter – with objectives)
2 – Conduct an initial risk assessment / survey – establish “RR”
   3 - Identify – your sensitive data – most have no standard
   4 – Classify – data according to its value to the organization
   5 - Discover & Map The Data – identify environment scope
   6 - Purge & Delete - Data that is no longer required

7 - Secure – employ security controls and protection measures (IAM, DLP, etc)
8 - Security Awareness & Training – employees are your first, and last line of defense… remind them and conduct frequent tests / exercises!
9 - Monitor – measure and evolve security & data practices.. (SIEM & DLP)
10 - Testing of Systems & Processes– assess and evolve security practices
11 - Establish & Practice Incident Response, it’s as important as data breach risk minimization!

Common sense steps for any data security, privacy effort

YET, how do we get there, the major activities to put in action?

So what’s a “RBSS” entail?

An integrated holistic approach to what matters most in our security efforts... three main thrusts:

Following NIST CSF & CIS CSC (1-8)
This is the essence of ‘cyber hygiene’ –along with vulnerability management

Manage / resource top risks mitigations (listed later)
Ideally use a 3rd party risk assessment, we’ll start with the risks listed herein

Using cyber threat intel (CTI), prioritize threat minimization
Continuous threat assessment, focused on phishing and patching (CIS 1 & 2)

Common sense steps for any data security, privacy effort
YET, how do we get there, the major activities to put in action?
Risk versus mitigation

Data loss / breach

Humans / Employees

Data protection gaps

Intruders / criminals

System Vulnerabilities

Weak Policy / procedures

Humans / Employees

Data protection gaps

Intruders / criminals

System Vulnerabilities

Weak Policy / procedures

Humans / Employees

Data protection gaps

Intruders / criminals

System Vulnerabilities

Weak Policy / procedures

Mitigations act synergistically between each other,
Generally: threat reduction lowers likelihood and data protection lowers the impact.

Key Cyber Risks

--- Data loss / breach (lost clients, recovery costs (several $M))
--- Failing compliance (fines, loss of trust, etc)
--- Ransomware / capabilities not available (lost productivity)
Where do threats come from?

OUR Threat categories:
• Rogue Employees
• Intruders / hackers
• System Vulnerabilities
• Data protection gaps
• Weak Policy / Procedures

Natural
• Fires / Floods
• Power failures

Unintentional
• Poorly trained administrators
• Accidents, inadequate policy, procedures
• Unaware or untrained employee

Intentional

Insider
• Fired employee
• Disgruntled employee
• Subverted employee
• Service providers
• Contractors / 3rd parties

Outsider
• Foreign intelligence agents
• Terrorists
• Criminals
• Corporate raiders
• ANYONE (using crime as a service)
How do threats act and propagate (e.g., cyber kill chain)

“cyber kill chain”
(Major protection mitigation inflection points)

1. Reconnaissance: Attacker gains information about the target.
2. Delivery: Attacker transmits payload via a communications vector.
3. Compromise/Exploitation: Attacker takes advantage of a software or human weakness to get the payload to run.
4. Infection/Installation: Payload establishes persistence in an individual host.
6. Lateral Movement /Pivoting: Malware moves through internal network to find and elevate privilege to valuable target.
7. Objectives/Exfiltration: Attacker accomplishes the attack (theft or damage).

Note – “hackers” exploit these threats using the cyber kill chain methods and “work flow.”
**ACTIVITIES**

**Data Breach Minimization**

- Encryption Assessment
- DLP Strategy & Project
  (Use Microsoft DLP Products, Implement Data Owners WG)
- IAM strategy / project
  (Use MS’ IAM products, with PAM, User PWs, certs, etc)
- VM Strategy / Project
  (Establish VM prioritization and integrate into CMDB. ‘MSBs’ set security posture)
- TVM / CTI strategy
  (Integrate SIEM, SOC. Other security tools; with industry CTI and company OSI)

**THEMES**

- **Data Protection**
  - Encryption
  - DLP and IRM
- **IAM** (Identity / Access Management)
  - Privileged / Insider
  - User PW quality
  - Remote access
- **Vulnerability Management (VM)**
  - ITAM/CMDB
  - “TVM” process
  - Fix critical issues
- **Intruder Detection**
  - Effective SIEM & SOC
  - Integrate Cyber Intel
- **Project Mgmt**
  - Awareness training
  - Risk management

**THREATS**

- Data Breach
- Ransomware
- Internal / insider
- Patching / Hygiene
- Hackers / Intruders
- Mobile Security
- “IoT” / Supply chain

**RISK BASED SECURITY STRATEGY = BEST RISK VALUE**
Building a Trusted Cyber Infrastructure
“= an adequately assured, affordable, net-centric environment”
(built from disparate heterogeneous capabilities that we must integrate into a homogenous cyber ecosphere!)

Focus on a few core capabilities & devices
= PC, routers, IA suite, Servers, & SANS – all with access control

Standard IA/CND suite
FW, A/V, IDS/IPS, CDS, VPN, Crypto, Key Mgmt, Security Policy

Security Monitor
HW / FW
Secure OS kernel
Secure Virtual Machine
Strict access / ZBAC
ALL OSes (MS, Mac, Unix)

Make IA / CND / Security a commodity:
Use & enforce IA building blocks = APLs/PPLs -> “NIAP”
Interoperability and Compose-ability are built in upfront
and help dramatically reduce complexity and ambiguity
Thus….establishing known risks & pedigrees:
Reduces attack surface, risks & TOC = baseline for PbD & IoT!
A cyber end-state stresses **encapsulation** using **secure communications**

(e.g., object oriented programming)
Data Security Centric view *(key aspects)*

Without question the **most heavy-lifting of GDPR compliance** (from a level of effort perspective) comes by way of Chapter 3 – **Rights of the data subject**. These are commonly referred to by the most well-known article (Article 17) as “the right to be forgotten,” but they contain far more data subject rights than the right to erasure. These data subject rights are extensive and include such rights as the **right of access by the data subject** (Article 15), the **right to rectify incorrect data** (Article 16) and the **right to data portability** (Article 20), among others. Make no mistake, enabling these data subject rights entails a substantial amount of work on IT systems and represents a significant amount of effort for many organizations.

Most legacy customer relationship management (CRM), electronic health record (HER), enterprise resource planning (ERP) and customer web portal systems simply were not designed to support these data subject rights.

Let’s take Article 20, for instance, which requires that data about a data subject be made available “in a commonly used and machine readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.”

The **data centric security architecture (DCSA) approach** defines some parameters for compliance and exceptions. DCSA alone can be a burden for extending existing business applications to enable compliance… Yet, **the long term benefits of DCSA are significant**.

Cyber Security opportunities
(Cyber can both protect your business AND enhance the bottom line!)

IT / Cyber Global factors – user pull

World-wide B2B
Trust / cloud / sharing

IoT / M2M
Automation / Sensors

Consumerization of IT
Phones / wireless / apps

Privacy / Data
IP / PII / compliance

GAPS / Needs
(from the Federal cyber priority council S&T gaps)

TRUST
Distributed / MLS

resiliency
SW / apps / APIs / services

agile operations
BE the vanguard / integration

effective missions
Business success factors

Vulnerabilities / Threats
(Verizon BDR, Forbes, etc threat reports - what ails us most)

CM / Hygiene
patching / settings

Access control
Authentication is key

TOP security mitigations
Whitelist, patch, limit access

Risk Mgmt
Global & E2E vs Adhoc

Future Opportunities

Effective Business Risk Management (BRM) = cybersecurity framework (CMMI / FAR)
Focus on reducing business risk… AI / ML of course = automation & cyber insurance …

SIEM / SCM
QA hygiene / sensors
“ESA” / simple tools!

Mobile Security
Poor apps / IOS weak billions users = volume

Mitigate Obsolescence
Minimize patching, legacy vulnerabilities OA / modularity / APIs & SCRM

Data Security
Predictive analytics
Privacy by design

Mike.Davis.SD@gmail.com