Minimizing Business Risk in Cyber security

An overview of the legal liability, technical issues and insurance aspects to help businesses mitigate risk
Reducing Business Risk

1 – **Be well prepared** - *Organizations MUST be at a ‘due diligence’ level of security protections* – the liability downside of not doing so is very real, and unfortunately happens every day to great companies and is very costly in every way! ($M)

2 – Get your Cyber environment *independently assessed (cyber baseline)* and then monitored – hire the experts, it’s faster & more complete (and adds to confidence level)

3 – Execute your *risk management plan*, fix the cost-effective vulnerabilities from #2, then *transfer risk on the unknowns*. Engage a cyber insurance broker to assist (AND counsel too)

Doing the right thing in cyber, is not hard, with the right help

Where by not acting, you are **gambling your business / livelihood**.
WHY should YOU Care?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average cost of data security breach:</strong></td>
<td><strong>$204 per compromised customer record per breach</strong></td>
</tr>
<tr>
<td><strong>Average cost per incident:</strong></td>
<td><strong>$6.75 million</strong></td>
</tr>
<tr>
<td><strong>Most costly breach:</strong></td>
<td><strong>$31 million</strong></td>
</tr>
<tr>
<td><strong>Least costly breach:</strong></td>
<td><strong>$750,000</strong></td>
</tr>
<tr>
<td><strong>Breaches at the service-provider level:</strong></td>
<td><strong>42% of all breach cases.</strong> These remain the most costly form of data breaches due to additional investigation and consulting fees.**</td>
</tr>
</tbody>
</table>
HOW BAD? Verizon Data Breach Report

2012 = 855 Incidents, 174 million compromised records, teamed with law enforcement
(this covers you too! report is a 6 year series, 2000 breaches, one billion compromised records – 36 countries)

WHO
- 98% from ‘external’ agents
- Mostly small business (over 75%)

HOW
- 81% Hacking
- 69% Malware

COMMON attributes
- 96% attacks not difficult
- 85% took weeks to discover (average is 416 days)
- 92% discovered by a third party
- 97% avoidable through simple or intermediate controls

Protect the palace
- implement a firewall or ACL on remote services
- change default credentials of POS and internet facing devices
- ensure essential controls met, regularly check them
- monitor and mine event logs
- evaluate threats to prioritize treatments

How BAD is the cyber security situation?
We have met the cyber enemy, and they are US
Ponemon: Negligent Insiders

The final analysis
YOU will be held liable at first, need to prove cyber ‘due diligence’
The Most Important Cybersecurity Case You’ve Never Heard Of

Wyndham’s challenge earlier this month in a case involving attacks by hackers on the hotel chain’s computer systems between 2008 and 2010. The FTC sued Wyndham last year for allegedly lax data security that let hundreds of thousands of credit-card numbers get stolen. In the current standoff with FTC, Wyndham Shoots Itself in the Foot.. As the FTC is going on the offensive in lack of data security .. Including more personal liability for company D&Os –this was cased dismissed, with prejudice… MORE to come!

The Securities and Exchange Commission (SEC) is pressing companies to be more forthcoming about attacks on their computer networks, and 47 states have enacted data-breach notification laws. Companies on the losing-side of data-breach class-action litigation pay an average settlement award of $2,500 per plaintiff, with attorney fees averaging around $1.2 million.

Idaho State University paid $400,000 to settle HIPAA security violations with the Office of Civil Rights. OCR contended that ISU failed to maintain adequate security by failing to maintain its firewall for ten months and for other systemic deficiencies. (re: lack of cyber hygiene)

3rd party “digital liability” – a huge costly unknown…
General Counsel’s Highest Concern

Survey results of 1,957 general counsel and 11,340 corporate directors at public companies:

• data-security is the most prevalent concern in 2012
• 33% of General Counsel believe that their board is not effective at managing a cyber attack;
• 58% of directors said that their company either had no formal, written crisis management plan for a cyber attack, or if they did, they did not know about it;
• Despite these figures, 77% of directors and general counsel believe their company is prepared to detect and effectively manage a cyber attack.
Insurance is *Transfer of Risk*

risk management = accept, mitigate or transfer

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

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

Source: Gartner

*Cyber risks* are pervasive – *are you covered*?
Basic Risk Reduction Perspective

What is the ‘real’ cost of cyber attacks / crime?
- Ponemon 2012 report = $8.9M / company (range 1.4 – 46M)
- McAfee 2013 survey = $400B / annually in US (down from $1T)
- Where piracy costs $1 to 16 billion annually, and drug trafficking $600 billion!

USE typical business success metrics (profit, growth, diversify, reputation)
- Doing the cyber security basics well, provides a 95% goodness level
- Plan your security programs around a ‘due diligence’ level of cyber

Major elements of an affordable, balanced risk reduction package
- KNOW your current as-is cyber security state – get an assessment baseline
- Ensure your risk management plan is current – covers all requirements
- Add missing key mitigations / programs the assessment recommends
- Effectively track and monitor key changes (SCM – security continuous monitoring)
- Use metrics to make decisions (tailor your big data analytics for cyber too)
- Partner with a cyber insurance broker and security legal team

Assess… fix key vulnerabilities...
quantify data / assess values… Insure…
WHY be more prepared in Cyber?

How much more evidence do you need???
- In recent events, Sony pays more than $171 million to recover from the PlayStation Network security breach where more than 77 million accounts were exposed.
- The overall cost of the Epsilon data breach in April 2011 could reach $4 Billion

Can your company afford even ONE major security breach?
The cost of a cyber security breach is measured by both “intangibles” and “tangibles” – the latter calculated using estimates of: - Lost business, - Lost productivity of the IT and non-IT staff, - Legal costs associated with defending yourself (even if “right”) - Public relations / consulting, - Increases in insurance premiums, etc…

You can not do this yourself / in house (versus using Independent Consultants)
- Need a third party evaluation….. Also… Independent Evaluations are required for environments with a “Moderate” or “High” Security Level as defined in NIST 800-53 CA-2.

There is a “due diligence” level of cyber security required…
don’t be the ‘low hanging cyber fruit’
Best values in reducing business security risks

Security assessment - know your ‘as-is’ risk state / posture = baseline
• 3rd party security readiness assessment (SRA) = much more than compliance
• Be protected to an accepted ‘due diligence’ level of security – follow NIST, etc
• Follow up with security continuous monitoring (SCM/SIEM) – keep track of cyber

Risk Management Plan – The C-suite has many risks, include cyber
• A RMP is a dynamic, proactive look / model of the business – not ‘shelf-ware’
• Quantify KEY risks, from authoritative sources – use data based decisions
• Do not let complexity trap you into analysis paralysis – be smart & DO something

Cyber insurance – the cyber ‘unknowns’ downside can be devastating
• Up to and including going out of business… and lingering liabilities as well
• Insurance is a risk management best practice – transferred to a third party

Where you have insurance for every KEY aspect of business… RIGHT…
Just as you have an umbrella policy for personal liability, so should you in cyber
Even “IF” you can prove ‘digitally right’ – court preparations = $10-25+K / case

It’s the integrated package that makes the difference!
Cyber Insurance Considerations
(before you select insurance, cover these factors (from Gartner))

Look past the initial the Sales Pitch – it’s not a simple transition (not the same as P&C)

Your current insurance broker and carrier may not be cyber current
There are around 50 now… re: Willis, Marsh, Aon, Lockton, also… Chartis, AIG, Beazley and Ace…

Cyber insurance policies are exceptionally complex.
Liability limits, exclusions – these must be studied carefully by risk, security and legal subject matter experts

Can the company provide "proof of insurability."
Organizations are required to complete a pre-insurance survey… provide data about policies, governance, perimeter security, access control, physical security and IT business processes.

Myriad of coverage options: breach, extortion, privacy liability, restoration…
Get specific coverage for understood gaps, rather than a broad set of coverage

Cloud and external IT services providers ‘not a given” reduction
They can create both a need and a limitation… Study clauses that cover errors or omissions – which could be used to imply that cloud services constitute a lack of acceptable protections.

Payment of Claims – Cyber insurance is still somewhat speculative
Insurance companies are using their own claims data — of which, they have little. Firms such as CyberFactors are using public data for loss data. Base your claim on a SRA – a quantified cyber level!

Our methodical approach minimizes these concerns
And makes them a PLUS in your risk management portfolio!
Is it Cyber Security ROI – or insurance?

ROI is a big deal in business, but it's a misnomer in security – it’s an EXPENSE!. Security ROI is difficult to compute, simply because it is hard to predict the probability of a true security event and the costs associated with the loss and mitigation of it. A major issue in cyber security right now is that we’ve never been able to construct an intelligent return on investment (ROI) for cyber security.

As we’ve never been truly able to gauge how big the risk really is.

But, you need to be able to gauge the magnitude of the risk. - what exactly the exposure is or if the actual event took place - because there just isn't enough good data... The classic gauge methodology is called annualized loss expectancy (ALE).

Cybersecurity ROI is considerably harder, as the threat morphs quickly - so we can't create ALE models. But there's another problem -- the math quickly falls apart when it comes to rare and expensive events - especially if the impact is huge, even low occurrence is costly.

Cyber ROI is misleading - as it is insurance – a cost of doing business

AND… You have insurance for every KEY aspect of business… RIGHT???
Cyber is NO DIFFERENT… In fact the ‘downside” can be loss of your business
Just as you have an umbrella policy for personal liability, so should you in cyber
Even “IF” you can prove ‘digitally right’ – court preparations = $10-50K / case

Cyber Insurance
don’t get caught in the cyber security legal quagmire without it!
NIST’s “*absolutely necessary*” Security activities

*NIST - National Institute of Standards and Technology*

- Protect information/systems/networks from **damage by viruses, spyware, and other malicious code.** (IA suite, A/V, etc)
- Provide security for your **Internet connection / ISP**
- Install and activate **software firewalls** on all your business systems
- **Patch** your operating systems and applications
- Make **backup copies** of important business data/information
- **Control physical access** to your computers and network components
- **Secure your wireless** access point and networks
- **Train your employees** in basic security principles
- Require **individual user accounts** for each employee on business computers and for business applications
- **Limit employee access** to data and information, and **limit authority to install software**

**MUST DO tasks**

consider this your main ‘due diligence’ list
Yet, even MORE cyber security guidance!

NSA IAD top ten controls

1. **Application whitelisting** - only run approved apps (that SysAdmin reviews)
2. **Control Administrative privileges** - minimize escalation, enforce least privilege
3. **Limit workstation-to-workstation communications** - thwart the “pass-the-hash”
4. **Use Anti-virus File Reputation Services** - leverage cloud-based threat databases
5. Enable **Anti-Exploitation Features** - for example, MS Windows EMET
6. **Implement Host Intrusion Prevention System Rules** - focus on threat behaviors
7. **Set a Secure Baseline Configuration** - layered security, standard images, etc.
8. **Use Web Domain Name Service (DNS) Reputation** - Screen URLs, intrusion alerts
9. **Use/Leverage Software improvements** - software / OS upgrade and patch policy
10. **Segregate Networks and functions** - based on role, functionality - monitor sections, then isolate when attacked

http://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf

NIST’s “Highly Recommended” Practices


- Policy / practice for email attachments and requests for sensitive information
- Policy / practice for web links in email, instant messages, social media, or other means
- Policy / practice for popup windows and other hacker tricks
- Doing online business and secure banking
- Recommended personnel practices in hiring employees
- Security considerations for web surfing, prohibited sites
- Policy / practice for downloading software from the Internet
- How to get help with information security when you need it
- How to dispose of old computers, media and fax machines
- How to protect against Social Engineering, data loss prevention

WHAT, “more to do?”

YES, but most are related to standard IA/CND mitigations...

Top 35 Mitigations

At least 85% of the targeted cyber intrusions the Australian Signals Directorate responds to could be prevented by following the Top 4 mitigation strategies:

- use application whitelisting to help prevent malicious software and other unapproved programs from running
- patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers
- patch operating system vulnerabilities
- minimize the number of users with administrative privileges.

**Examples of Targeted Cyber Intrusions mitigation strategies**:

- Disable local administrator accounts; Multi-factor authentication; Network segmentation and segregation; Application based workstation firewall; Host-based Intrusion Detection/Prevention System; Centralized and time-synchronized logging; Whitelisted email content filtering; Web domain whitelisting for all domains;
- Workstation application security configuration hardening: User education; Computer configuration management; Server application security configuration hardening; Antivirus software with up to date signatures; Enforce a strong passphrase policy; ETC; Etc; etc.


SANS top 20 controls (ver 3)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on the Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

http://www.sans.org/critical-security-controls/
Regulatory Requirements

• State Breach Notification Laws
• State Data Security Requirements
• Gramm-Leach-Bliley Act ("GLBA")
• FTC Section 5
• SEC
• Health Insurance Portability and Accountability Act ("HIPAA")
• EU Data Protection Directive
• Congress considering bills to establish national notification requirements
Texas: Reaching Beyond the Boot

• Thanks to a 2011 amendment to the Texas reporting law, if you “conduct business” in Texas, not only must you notify Texas residents (if any) that their data has been breached, but you [may also] have to notify residents in states that have no breach disclosure laws, or face potential consequences from Texas.

• That is, the Texas reporting law theoretically includes all US residents!

• This is but ONE example, where keeping track of all the cyber / digital / privacy laws is almost impossible…inside the USA, let alone international Thus again showing the criticality of effective cyber preparedness / proven due diligence level… especially in 3rd party suits – which can come from anywhere at anytime! And will get worse globally…
Getting Counsel Involved

- Preliminary Retention and Incident Response plan
  - Management will always have many questions.
  - How did it happen? Is it still happening? Could it happen again?
  - Did the incident actually occur (did we actually lose data) regardless of what particular people think.
  - Exactly what data was stolen? Do we have third party liabilities?
  - Do we have definitive evidence to support those answers?
  - Who was involved? Internal or External? Who have we notified (CERT, FBI, etc)
  - Can we get restitution? Can we effectively prosecute them.
  - What else would our organization need to know to minimize liabilities and reputation damage?
  - If we end up in court or in front of a regulator, how are we going to prove our case, and who’s going to testify?

- Retain forensic investigator “digital evidence” and wrap in privilege
- A Trusted Advisor is essential where litigation is anticipated or inevitable
Cyber process for **Insurance** (et al)
(a simple method to manage cyber ‘complexity’ iaw your **RMP**!)

The below illustration is a general guide to how the cyber risks can be quantified, using authoritative sources and methods, into quantifiable risk levels to ACT on, and then insure

**Security Risk Assessment (SRA)**
(several levels, remote, onsite, etc)
(Check only key points, or compliance levels, or business tailored, etc)

Environment is scanned
Key IA/CND settings assessed
**level of security assessed**
(using NVD CVE, etc)

**Security Continuous Monitoring (SCM)**
(monitor ‘hygiene’, access, unusual behavior - cyber mgmt informed)
(status files sent to central Sec OpsCtr)

Security OpsCtr assesses data
- Changes in key IA/CND settings
- Abnormal patterns (SIEM)
- Adjusts security level based on changes and thresholds
- Feeds security actuarial tables
- Alerts sent to multiple entities
- Validates compliance aspects too

**Assess property value (IP & real)**
(quantify and value data / IP)
(identify other IT / property / assets)

User does inventory (data & IT)
*puts dollar value on key items* (see “SDIM” effort on IP value)
Matches mitigations to RMP
Quantifies the ‘known’ and bounds the ‘unknown’ aspects

**Cyber Insurance**
(contact cyber ins broker)
(team with legal firm)

Broker uses **cyber actuarial tables**
Maps security levels and assets values
Premiums based on both (and deductibles)

All processes are linked – with feedback between analytics
(aka, *user based behavior insurance* as risk takers = higher premiums)

**SRA / SCM + insurance = due diligence = major risk / cost reduction = profit**
Cyber Level: Baseline + Hygiene + Analytics
= integrated cyber package = operate lowest risk -> cyber insurance!

**Baseline**
Assessment
(know the as-is state)

- **Mitigate** key vulnerabilities
  (RoI / affordable)
- **SCM / SIEM monitoring tools**
  (hygiene & audit)
- **Training** (NICE) &
  **Process** (“CMM”)
- **Privacy State**
  (assess, monitor, etc)
- **Open source Intel assessments**
  (who are YOUR threats)

**Known residual risks**

Assess, quantify the relative security level
(with common metrics)
= (CVE / NVD)

Basic known unknown risks

Minimizes unknown unknown risks

1 + Monitor for insider threats
(and SCRM…)

2 + **Open source Intel assessments**
(who are YOUR threats)

- **(Define)**
  Apply To standard ‘cyber’ actuarial table

- **AND**
  Supports the NIST / White House cybersecurity framework!!

- Insurance industry MUST have a common assessment process
  Then use a standardized cyber security actuarial table, to further provide policies without extensive exclusions, AND cover privacy too

And WHEN (not if) you suffer a loss, consider / factor in the bad actor source too,
As all the due diligence in the world, likely won’t stop the best hackers there are
A mitigating factor is “I did all I could” – the best hacker there is got to me, it’s like an act of God.
Cyber Actuarial Table Factors

The major security elements / factors that matter to a cyber outcome are:

(1) - Security baseline quantified
with mitigations applied where cost effective) – provides the security environment status / state.

(2) - SCM / SIEM / monitoring tools and methods
when a baseline goes out of tune, this tracks it, also catches trends, etc…

(3) – Security Policy
an effective security policy must be in place, communicated from the top, periodically updated and enforced

(4) – Cyber Processes
guidance with documented methods (SoPs) are required to standardize behavior (e.g., CMMI)

(5) – Training and education
Once 1-4 are in place, users / operators must have adequate skill levels

(6) - Privacy state - mandates / LAWs with fines, etc…
Data breaches and loss of IP are huge risks, with extensive 1st & 3rd party liabilities

(7) – Monitor for insider threats
a known threat vector to be proactive on – monitor for unusual behavior for people AND things (SCRM)

(8) – Intel assessment on organization
OSINT - know your enemy – then guard against their typical attacks
How’s the process work?

+ Using existing authoritative sources on what thresholds matter in each capability (1-8), Clients self-assess their status and use that as a discussion tool with broker.

+ The Broker takes the clients assessment and provides their perspective, based on their own level of knowledge in the relative security posture, due diligence aspects, level of assessment (self versus SME), etc to come up with a confidence factor

+ The broker applies confidence factors to each element for a normalized value

Makes recommendations to the client on cost-effective mitigations to reduce risk.

+ This allows both parties to come to a more formal agreement on the cyber posture, and any added measures to reduce risks, minimize exclusions and lower premiums.

<table>
<thead>
<tr>
<th>Category</th>
<th>range</th>
<th>Thresholds (and existing risk levels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred</td>
<td>0.85 – 1.0</td>
<td>1-5 factors are H, 6 &amp; 7 are in work at some level, no known M or higher risks</td>
</tr>
<tr>
<td>Above Average</td>
<td>0.70 – 0.85</td>
<td>1-5 factors are mostly H, with #1 H, #6 is in work, no known H, 1-2 M risks</td>
</tr>
<tr>
<td>Average</td>
<td>0.55 – 0.70</td>
<td>1-5 factors are all M or higher, no known H risks, some M with mitigations</td>
</tr>
<tr>
<td>Below Average</td>
<td>0.4 – 0.55</td>
<td>1-5 factors are close to M, any high risks are managed, POA&amp;M for others</td>
</tr>
<tr>
<td>High Risk</td>
<td>0.0 – 0.4</td>
<td>1-4 factors are below M, unknown baseline, existing high risks – “sitting duck”</td>
</tr>
</tbody>
</table>

**EXAMPLE** Risk impact table – which is then applied to digital assets according to insurer methods.

The cyber security actuarial table is then a common discussion tool!
How’s the process work?

Each element is assessed by the client for a ‘security status’ using thresholds established by authoritative references, then a value is generated (“S” - initially H, M, & L). Assessed with common, accepted tools / methods to measure the status and state of the element. The “S” level is then justified in the “rationale” column, where the comments column is then used for mitigations, extenuating circumstances, etc.

The broker applies the confidence aspect of the element, to arrive at a risk weighted value level (“V”) which is the level that relates to the risk category.

<table>
<thead>
<tr>
<th>Element</th>
<th>W</th>
<th>S</th>
<th>V</th>
<th>Rationale / level (= justify ‘S’ #)</th>
<th>Comments (mitigations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security baseline</td>
<td>0.35</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>SCM / monitoring</td>
<td>0.15</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Security Policy</td>
<td>0.075</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Processes (SoPs)</td>
<td>0.075</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Training &amp; education</td>
<td>0.1</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Privacy State</td>
<td>0.15</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Insider detection</td>
<td>0.05</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Company Intel</td>
<td>0.05</td>
<td></td>
<td></td>
<td>H - M - L</td>
<td></td>
</tr>
<tr>
<td>Aggregate score</td>
<td>(1.0)</td>
<td>---</td>
<td></td>
<td>Weighted / normalized total</td>
<td>Used to enter risk level chart</td>
</tr>
</tbody>
</table>

The cyber security actuarial table is then a common discussion tool!
WHAT to do next
When you return to the office

* Work with your IT/Cyber Professionals – get a SME / MSS
  (Find a security partner - Follow the cyber security best practices!)

* Enforce your Information Security Policy!
  (it should also address how any outsourcing with vendors is handled)

* Verify you are ‘actually’ in compliance & monitor
  (DO “SCM / SIEM” - and keep up with changing liability / laws)

* Require effective risk & security training for employees
  (incentivize too – for sales people, IT, managers... acceptable use of IT assets like USB drives, printed documents – using a shredder?, reporting suspicious behavior, - who is working remotely? )

* Partner with KEY risk managers ASAP:
  (1) your broker/Ins company, (2) Law Firm and (3) Cyber Security Expert.

Quit just admiring the problem / threat and “DO” at least one thing TODAY!