CISO Fundamentals *(Cybersecurity tenets)*

Getting back to the cyber basics, stabilizing the environment.

The urgent need for a unified cyber security protection profile is highlighted by recent high profile reports of companies being hacked (SONY, et al), critical infrastructure being compromised, intellectual property (IP) being stolen, and the rise of ransomware ("CryptoLocker"). Companies are realizing the risks associated with the loss of IP/data, money, privacy, and tarnished reputation/brand name from cyber-attacks are *intensifying and accelerating* in today's hyper-connected environment. These risks include disruption of business operations, data corruption, leakage and theft, significant financial and legal liabilities, and loss of customer base. The role of the Chief Information Security Officer (CISO) is to remain vigilant on the cyber fundamentals: malware outbreaks, minimizing data breaches, protecting data and assuring company and customer privacy, continuous monitoring of networks, and risk management. When small businesses don't have a CISO, these risks and their impacts are more amplified in day-to-day operations, cash-flow, clientele, business reputation, among others.

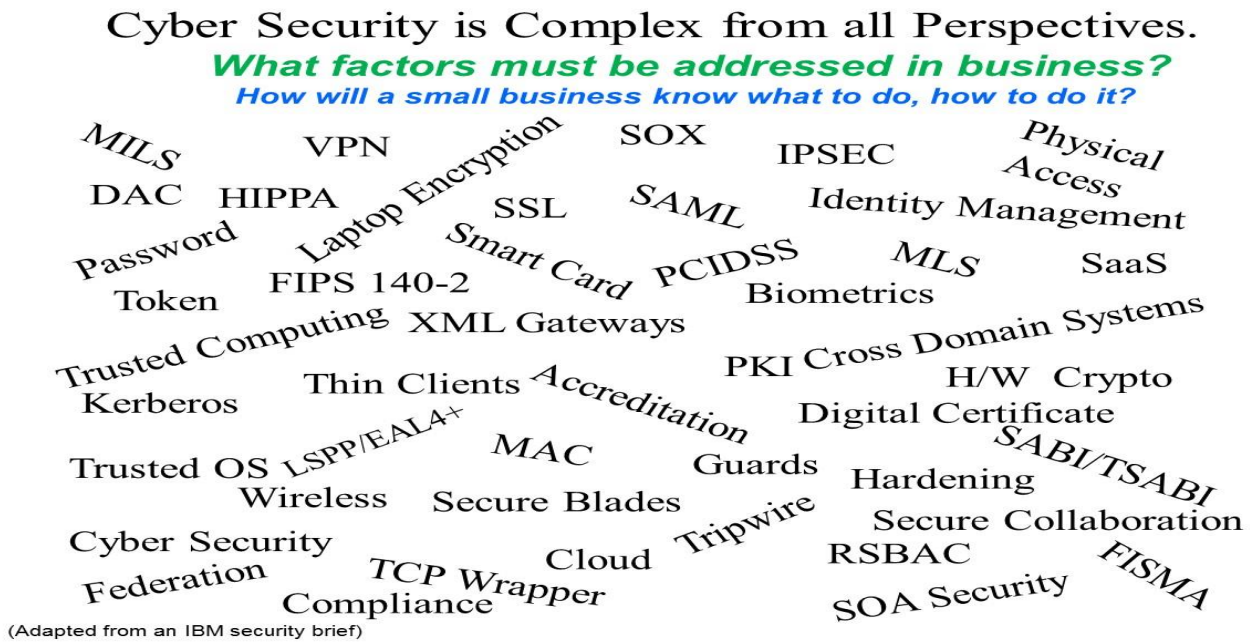
The need for a common cyber profile raises a few questions: "what are the key cyber protections to implement?" and "can we afford to implement them?" *We say the answer is YES, using an overall risk management approach and following the recommendations below*. This article proposes an effective and affordable path to implement an adequate and well proven level of cyber security operations. The security threats we presently face are very real. The news only shows the high visibility attacks (Target, JPMorgan/Chase, Ebay, Home Depot, etc), and leaves out the fact that on average we will all eventually be breached (or already have been and don't know it yet). Therefore, we believe that businesses must understand they cannot buy cyber security, instead they must manage their cyber ecosystem using the "5Ps" of any endeavor = people, processes, policy, product and now privacy, too.

The standard cyber security suite today can be effective, if maintained, enabling business owners to focus on business operations, mitigating critical risks, protecting privacy and minimizing legal liabilities. We recommend organizations stay current on cyber threats and mitigations by associating with their business sector Information Sharing & Analysis Centers (ISAC), the local FBI outreach, and US-CERT. Two representative threat summaries highlight the need for effective cyber protections.

FORBES magazine listed key security vulnerabilities as: *social engineering, advanced persistent threats, internal threats, bring your own device, browser based attacks, botnets, targeted malware*, and *the cloud.*

The 2014 Verizon data breach report's top threats were: *point of sale intrusions, web application attacks, cyber espionage, card skimmers, insider misuse* and *crime ware*.

The threats these organizational reports list can seem overwhelming, and the complexity of the many types of cyber capabilities and functions (illustrated below) can look daunting, but <u>the cyber solution to minimizing over 90+% of most security incidents is implementing the security basics, and doing them well</u>. *Know, stabilize, maintain, and monitor your security baseline, cyber environment, within a proactive risk management ecosystem*.



(Adapted from an IBM security brief)

Best practices in organizational protection use a balanced cyber security approach within an enterprise risk management framework accommodating the "5Ps." Since nearly all security incidents are associated with NOT doing the security basics (e.g., keeping product settings and patches current, effectively controlling data/network access, etc.), companies must implement a security continuous monitoring (SCM) capability to watch for and manage any improper settings and scan for abnormal behavior. The organization's risk management plan (RMP) is another critically important tool to balance risks, resources, and priorities to support the key mission essential functions of the business. For the business sector, there are many security guides that offer best practice security controls (including: keep software updated, educate employees, monitor social media, employ effective passwords, limit access to sensitive data, and control downloaded apps). The CISO must understand, integrate and efficiently manage all these controls, providing affordable, effective protection to all stakeholders.

The balanced and integrated security approach premise we promote is that companies can be well protected (to at least a notional due diligence level) based on implementing a few key guidelines:

(a) NIST SP800-53A (rev 4) 'security and privacy controls' and specifically their NISTIR 7621 (Rev1) "SMB Security" – with the "absolutely necessary & highly recommended" actions therein, and

(b) Both the NSA top ten and SANS top 20 security controls.

These sets of controls collectively define a defendable *"due diligence" security posture*. The business environment needs to maintain a high infrastructure and data protection profile, with effective SCM, while not encumbering the users' productivity. Embed the following cyber tenets into your RMP for maximum protection:

- Employ well proven security products, which entails at least: anti-virus, firewall, VPN, IDS, encryption (with robust key management) and SCM (note - buy security programs from only formal, approved product lists).
- Continuously manage, monitor, mitigate and automate your IT/security baseline (use tools, dashboards) – *the key here is "visibility" – KNOW your security environment* - as you can't manage what you don't see.
  ***These five activities can reduce security incidents by well over 90%*:**
  - Effective application upgrade and patch management (track and prioritize business apps);
  - Controlling network and data access (enforce "least privilege" & *minimal privileged accounts*);
  - Application whitelisting / secure configurations (software certs needed to execute);
  - Current hardware and software inventories (with the current versions / IOS / patches); and
  - Employing SCM / SIEM (on premise and the cloud – *effective monitoring SLA*s).
- Secure backup is paramount, using multiple locations – most storage should be encrypted, and address cloud security in SLAs. **Encrypt all data** at rest and data in motion (internet / wireless / external connections).
- Manage access to the company, both physical and virtual - use strong passwords, changing periodically (not too often) - consider a token/biometrics for sensitive data. Strictly limit "privileged access."
- *As IP / data defines your business, focus on data security, privacy by design* – categorize it and know where it is – use "Data Loss Prevention / Data Rights Management" to manage access and track key data.
- Proactively manage business risk using your RMP, complemented with a well-communicated, enforced security policy. Use a cyber insurance policy to transfer known accepted and unknown risks - base coverage on a risk assessment (ISO 27000 series) – use the policy to harmonize management, broker and counsel.
- Robust resiliency and recovery – have a Business Continuity Plan – and an incident response plan.
- Provide ongoing training and education on security awareness and business risks, tailored to all key stakeholders. Make the training personal, with natural work applications, as it will last longer.
- *KNOW your security status / metrics* – periodically, independently test and assess the: security suite, ongoing processes including back-ups, security policy enforcement, and all major elements in your RMP.
- What about forensics, ethical hackers, etc – of course, just do the basics well first, then work damage control.

As business leadership becomes more cyber aware, a CISO must be able to translate the above overall cyber tenets into "C-suite language" – operational impact, costs, revenues, value and market share (brand, etc).
A CISO will typically have to fulfill these requirements with minimal resources, so they must be creative in implementing an effective, affordable cyber ecosystem, all while *making cyber and privacy business enablers*!
By implementing these cyber tenets, a CISO can be more than just a cyber cop, privacy enforcer, and excel as a value-added risk communicator throughout the organization, from the C-Suite to the shop floor.
To efficiently imbue effective and affordable cyber security and privacy into your business and enhance the value proposition, *contact Mike at* **Mike.Davis.SD@gmail.com** and *Gary at ghayslip@gmail.com*.
For a more detailed overview on a '*Cyber model for Privacy by Design*" and "*Executing an effective security program*" AND many *other cyber and privacy resources* - see **http://www.sciap.org/blog1/?page_id=1184**