SECURE THE VILLAGE
Creating CyberGuardians

CybersecureAmerica 2021
A Reasonable Approach to Reasonable Security, the Sequel
October 21, 2021

Computing Your Information Security Risk Profile

Section 1: Understanding Your Threats. Cataloging Your Risk

The following table identifies several attack types that threaten your organization. Given your particular organizational circumstances, indicate whether an attack is expected or unexpected. You should expect to implement information security practices to effectively – and cost-effectively — mitigate these threats.

Threat of Attack	Expected / Unexpected / Don't Know
Business Email Compromise	Expected
Ransomware	Expected
Cyber Extortion	
Theft of customer *Personally Identifiable Information* (PII)	
Theft of Intellectual Property	
Network breach	
Website breach	
Website Denial of Service	
Operations Denial of Service	
Sabotage of your network by competitor or outside enemy	
Sabotage of your network by a disgruntled employee or contractor	
Attack by a nation-state	
Attack by a political enemy	

The following table identifies several legal obligations to which your organization might be subject. Indicate whether you are subject to the indicated legal obligation. You should expect to implement information security practices to effectively – and cost-effectively — manage these obligations.

Legal Obligations	Applies (Yes / No / Don't Know)
Must notify consumers in event of breach	
Must notify SEC in event of breach	
Subject to health care privacy regulations (HIPAA)	
Subject to financial services regulations (Gramm-Leach-Bliley)	
Subject to FTC Safeguards Rule	
Subject to Payment Card Industry Data Security Standard (credit cards)	
Subject to CA Consumer Privacy Act (CCPA)	
Subject to other state privacy laws	

Subject to EU GDPR	
Subject to other nation's privacy laws	
At significant risk of lawsuit by customers in event of a breach	
At significant risk of lawsuit by trading partners in event of a breach	
At significant risk of lawsuit by shareholders in event of a breach	

The following table identifies several competitive requirements to which your organization might be subject. Indicate whether you are subject to the indicated requirement. Also indicate if you might have a competitive advantage over competitors whose information security practices are not up to the competitive requirements. You should expect to implement information security practices to effectively – and cost-effectively — manage your requirements while giving yourself the opportunity to take market when it becomes available.

Competitive Requirements	**Applies (Yes / No / Don't Know)**
Covered by CMMC (Cybersecurity Maturity Model Certification)	
Required to comply with information security practices set by customers / clients	
At significant risk of losing customers / clients in the event of a breach	
At significant opportunity of gaining customers / clients in the event a competitor has a breach	

The following table provides identifies special circumstances that can impact the complexity of your information security management practices. Information security management can be expected to become more complex as size, number of locations, etc increase.

Size and Complexity	**Answer**
How many employees / Staff do you have (< 100; 100<x<1,000; >1,000)?	
How many office locations?	
What % of staff work remotely?	
Is IT in-house or outsourced?	
What % of deliverable work is performed by subcontractors?	

Section 2: Calibrating Your Risk Tolerance

Work through the following scenarios. They are designed to help you calibrate your information security risk by answering the question "*What can I afford to lose?*".

Combined with the last question asking about your general risk tolerance, this Section will help you calibrate the information security risk you feel comfortable taking on.

Scenario 1: A cyber attack prevents you from serving customers / clients.

1. How long could you be down before it would begin to hurt?
2. How long could you be down before it would be painful?
3. How long could you be down before it became catastrophic?

Scenario 2: You are defrauded by Business Email Compromise.

1. How much could you afford to lose before it would begin to hurt?
2. How much could you afford to lose before it would be painful?
3. How much could you afford to lose before it became catastrophic?

Scenario 3: A cyber attack compromises sensitive information of your customers / clients.

1. What information – and how much of it – could you lose before it would begin to hurt?
2. What information – and how much of it – could you lose before it would be painful?
3. What information – and how much of it – could you lose before it became catastrophic?

Risk Tolerance: Which of the following best describes you:

1. I am very risk averse. I prefer safe bonds to risky stocks.
2. I am moderately risk averse. I prefer a careful balance of stocks and bonds designed to provide a stable annual return.
3. I like to roll the dice, the thrill of the chase, betting on a big winner.

Section 3: Your Information Security Management Practices — Surveying Your Defenses

Below are 25 information security management practices; defensive measures designed to lower the likelihood of a successful breach, help you comply with your legal responsibilities and customer requirements, and potentially allow you to gain market share from the misfortune of competitors.

As can be seen, some of these practices are strategic, others are tactical, and others are both.

For each measure, write "Y" if you currently implement the measure and "N" if you do not implement the measure. Also indicate if you don't know whether your organization is implementing a particular practice.

The number of "Yes" answers is a measure of the strength of your information security program.

Twenty-Five Information Security Management Practices	Strategic Importance	Tactical Importance	Yes / No / Don't Know
We have a named executive responsible for information security management.	✓		
We have an information security program based on a framework such as the NIST Cyber Security Framework, the Center for Internet Security Controls, ISO 27001, 02, or similar.	✓	✓	
We have qualified operational expertise in information security / privacy management.	✓	✓	
We have provided awareness training to all staff in the last year.	✓	✓	
We have an active program to create a cybersecurity adaptive culture.	✓		
Our IT Team has an up-to-date inventory of all our hardware, software, and cloud services.	✓	✓	
Our IT team has deployed, maintains, and automatically updates our anti-malware defense	✓	✓	
Our IT team updates and patches all operating system and applications at least monthly.	✓	✓	
Our IT team has an active vulnerability management process that includes a network vulnerability scan at least monthly.	✓	✓	
We use Multi Factor Authentication (MFA) for email access.		✓	
We use Multi Factor Authentication (MFA) for access to online financial accounts.		✓	
Our IT team encrypts all data "in transit" and "at rest" on workstations, servers, and in the cloud	✓	✓	
Our IT team has securely configured our network with firewalls, network segmentation, and other appropriate configuration and change management controls.	✓	✓	

We maintain offline backups and test their recovery at a documented frequency, at least annually.	✓	✓	
We have documented Incident Response and Business Continuity Plans that are updated, trained and tested at least annually.	✓	✓	
We have an active data management process that includes a current up-to-date inventory of all our sensitive information and a list of users authorized access to the information.	✓	✓	
We review our information security posture with Executive Management at least quarterly.	✓		
Our IT Team securely maintains at least 90 days of audit logs of sensitive network activity.		✓	
Our IT network requires all remote access to be by means of a VPN with Multi Factor Authentication (MFA).		✓	
We have an active Vendor Risk Management Program to assess and manage the risk to us of a cyber-attack on our IT vendors and technology service providers.	✓	✓	
All fax and email requests for funds transfers are verified by a phone call to the intended recipient.		✓	
We have had an information security review and assessment by in an independent 3rd-party in the last 12 months and are actively working to remediate its findings.	✓	✓	
Our attorney has reviewed our legal exposure in the last year and we are actively working to implement their recommendations.	✓		
We review our risk exposure with a qualified cyber-insurance broker at least annually	✓		
We have cyber-risk insurance covering 1st and 3rd party risks.	✓		