Management guide
for fighting
cyber predators

Table of Contents

Introduction

Our objective is to provide structure and guidance to those who wish to protect themselves and their organizations from the predators that are present in cyber space. Our approach has three basic assumptions:

1. Known cyber risks are immediate and real threats. They need to be addressed and dealt with on an on-going basis. They cannot be ignored. And one must be ready to deal with the new cyber risks that arise. Unfortunately, this means you will always be playing 'catch-up' as new risks arise daily. Leading to what we call playing 'cyber wack-a-mole'.
2. If you wish to stop playing 'cyber wack-a-mole' you need to implement a parallel approach that deals with your cyber exposures and cyber security culture.
3. Many organizations, faced with resource (staff, dollars and technologies) constraints, may require a segmented approach.

If you accept these assumptions then you need to maintain, or even improve, your present cyber security efforts while developing and implementing a strategy to get out of the cyber wack-a-mole situation. This realization can be over whelming considering the complexity and size of the potential issues involved.

Agreed.

Which is why we developed this guide. You need a strategy to deal with the complexity and magnitude of the cyber security issues you face. . We call it 'strategic segmentation'. That is you need to break your situation into segments that can be dealt with within your available resources.

First and foremost you have to continue with your cyber security efforts. We will detail some steps that, if you are not already taking you should consider.

Second we will present some thoughts on how to decide on what segments are appropriate for your organization. As part of this we will examine the following possible segments in some greater detail.

- Cyber Exposures (vs cyber risks)
- IoT
- Cyber Security Culture
- Regulatory Environment
- Cloud Computing
- Social Media
- Privacy
- Education

Third we will offer some thoughts on how an organizations approach to cyber security will vary by size. There are different strategic considerations for small, medium and large organizations. Note we think the distinction between local, national and international organizations is losing relevance as cyber space is not defined by geography.

Finally we have included links to resources and sites that offer education, information and guidance.

Existing Cyber Security Efforts

We assume you have a cyber security program in place. If you do not have an existing cyber security program stop reading and develop and implement such a program. Once you have one in place then come back and continue.

For an existing cyber security program we strongly recommend you make sure your program includes the following:

- Written cyber security policies and regulations that you publish and distribute to all employees, vendors and contractors.
- Education regarding your cyber security policies and regulations that is required of all members of your organization, including senior executives, vendors and contractors.
- Making sure all default settings and vendor supplied passwords have been changed from those initially supplied.
- Sensitive information[1] that you handle, process or store is identified, responsible party identified, protected by encryption and access controls? Are they monitored?
- Backup copies for all organizational data, especially sensitive data, made on a regular basis with off-site, secured storage.
- Do your disaster recovery/business continuity plans (DR/BCP) include sections covering your cyber eco system, its many components, it recovery and continuing operation should an unforeseen event occur.
- Your normal operating procedures should include change management and configuration management processes. The detail documentation should include who is responsible and how that individual will be monitored and managed.
- Firewalls that cover outbound transmissions as well as inbound.
- Wiping clean all devices and materials disposed of. This includes copiers, printers, cell phone, other intelligent devices as well as the usual hard drives, pc's and laptops.
- Both physical and electronic intrusion detection and monitoring.
- BYOD policies and procedures

This list is not meant to be exhaustive, rather indicative of the details that your existing cyber security plans should include. To assure a high level of confidence in your cyber security plans and programs we recommend you have an outside expert conduct a review to uncover any deficiencies.

[1] Sensitive information includes but is not limited to personal identifiable information, proprietary organizational information, and other sensitive information.

Strategic Segmentation

The following list provides thoughts on tasks and actions that can be pursued individually if a full scale program is not a viable option at this time. The order they are presented in does not reflect importance as what is the most important will be the ones that benefit your organization the most and only you can determine segment priority.

Managing Cyber Exposures (vs cyber risks)

We hear a great deal about rising cyber threats. It seems every day a new cyber threat arises, which leads to a great deal of activity to determine how to react to it. This is a strategic mistake. Focusing solely on cyber threats is a losing proposition as there will always be a new cyber threat to deal with, it is technologies version of cyber 'wack-a-mole'. You need to stop playing cyber wack-a-mole and begin to take the offensive against the predators that infest the cyber eco-system we all inhabit.

Instead what you need to do is to identify and manage your cyber exposures so you are not always playing catchup. That is not to say you should ignore cyber threats. You need to deal with ones that are prevalent in your cyber eco-system. Rather, you need to also, if you want to get ahead of cyber threats, identify and deal with your organizations cyber exposures. By 'cyber exposures' we mean the vulnerabilities that arise from inhabiting the cyber eco-system. You need not be doing anything exotic or leading edge just use computers, smart devices, networks and the Internet and you are in a cyber eco-system that has predators hunting for vulnerabilities. Realize that these vulnerabilities are not just technical but rather are rooted in human behavior, legal and compliance matters, use of social media, the cloud and the Internet of Things (IoT).

You need to identify as near as possible all your cyber exposures. You need to know if you have major cyber exposures and so that you can begin to prioritize and address them. If you are not aware of all your cyber exposures then you will be defending your organization from the known threats while leaving major access paths into your organization for predators to exploit. And the predators are like most people, they will go for the easy prey.

To accomplish this you need to understand how to identify your cyber exposures and then understand how best to manage those the you have found. We suggest that to do this, if you do not have the current knowledge and ability, you can either take our course, 'Managing Cyber Exposures' available on the Global Risk Academy (see the links section for the URL) or consult an outside expert.

Internet of Things (IoT)

The Internet of Things (IoT) consists of all the intelligent devices and systems that are connected to your network and thence to the Internet. They can represent a wide open door into your organization if not secured.

The problem arises in that many of the devices have minimal security and are installed using default settings, which are known to the bad guys out there. And in many cases the installations occurred with no coordination with IT or security functions, as they are, other than the network connection, independent devices paid for and used by business functions for managing their specific function. And in many cases needed only the approval of their management chain, so no one else knows they are there.

Some of the places IoT devices may reside are building control systems (HVAC, UPS, electrical distribution, lighting systems, elevators, or similar systems.), process control systems (manufacturing lines, machine tools, chemical processes, ovens, and the like), automated warehousing/distribution systems (automated picking conveyor systems, loading and unloading systems and equipment such as forklifts, or similar systems), intelligent equipment or devices (such as phone systems, office copiers, fax machines, scanners, communication systems, intercoms, or like devices), and building services including those that process maintenance requests and tracking, managing building control systems, scheduling building resources, managing visitor traffic, or the like.

For each IoT device found you need to inventory the specifics, including the responsible party, determine what security, if any are in use, make sure the operation is monitored, audited and tested on a regular basis to assure safe and secure operation.

Cyber Security Culture

A key to successfully addressing the many cyber exposures your organization faces is understanding the mindset of the members of your organization – the cyber security culture. This can be done by examining attitudes towards cyber exposure, responsibilities towards cyber security, and awareness of the cyber threats in general. In other words how does your organization view cyber security? Is it only a technical concern? Not a real problem? An annoyance to be circumvented? The answers to these and similar questions will go a long way towards understanding the approach you take to improve your organizations cyber defenses. If your culture treats cyber security poorly then your organization is much more likely to experience a cyber event.

You may wish to consult with experts in the field of culture management, or we have included a link to our Cyber Security Culture Barometer which is free, and can provide some initial guidance.

In summary: cyber security culture matters and cyber security culture can be managed.

Regulatory Environment

You need to, with the guidance and advice of a trusted legal advisor, review your cyber operations to make sure you are in compliance with all the regulations that apply to your organization. This is not a simple task since many jurisdictions have unique regulations that may apply and if you have a presence on the Internet you may inadvertently be operating within jurisdictions and not know of it.

In addition you need to make sure you are in compliance with supra national regulations that may apply should you process credit cards. Specifically the Payment Card Data Security Industry Standard (PCI DSS). Others may apply which is why you need to enlist a trusted legal advisor to determine what applies.

Cloud Computing

Use of cloud services for data storage and processing is growing and brings cost benefits which can lead to entry into agreements that do not reflect the necessary security and other protections. First you need to determine if any such agreements are in place in your organization and then make sure they consider the following.

Whether your organization's data will be stored only in your home jurisdiction to resolve any jurisdictional issues in the event of a dispute with your provider; and the financial stability of the provider, including reviewing third party audit reports of the provider's security and privacy practices, a copy of their cyber liability insurance, the results of internal audit reports, a copy of the provider's Disaster Recovery/Business Continuity plan and the results of the latest comprehensive test of this plan.

The following items should be discussed in any contract you agree to:

- where your transactions and data will be stored and how you can remove them, and at what cost
- how the removal of your company's transactions and data may be moved from the provider, including the security and cost of such a move;
- what kind of security safeguards will the provider apply to your transactions and data
- what terms of limits of liability is the provider imposing on the transaction
- who will control breach incident response and bear the cost
- whether the provider will indemnify the organization and, if so, under what circumstances

You need to also find out whether your cloud provider does the following:

- conducts network penetration tests of its cloud service infrastructure regularly as prescribed by industry best practices
- Segment and recover transactions and data for a specific customer in the case of a failure or data loss
- Sanitizes all computing resources of your transactions and data once you have ended the arrangement
- Provide documentation that sets out the process and rationale for moving transactions and data from one physical location to another
- encrypts transactions and data at rest within its environment, and that in transit
- has anti-malware programs installed on all systems that support the cloud service offerings?
- maintain logs for traffic monitoring and auditing including who accessed your account, what they accessed and how long they were logged in

Privacy

There are several keys to addressing cyber exposures arising from privacy concerns. They are:

- Identifying all the sensitive information[2] that resides in, or is processed by your cyber eco-system along with the responsible party for that information.
- Making sure such sensitive information is secure, monitored and audited at all times.
- Making sure such sensitive information does not leave your facilities unless secured and a responsible party identified. This includes staff intelligent devices used for work purposes, the disposal of equipment, and off site storage.

[2] Sensitive information includes but is not limited to personal identifiable information, proprietary organizational information, and other sensitive information.

Education & Communication

Key is that you have a set of cyber security policies and procedures that you distribute throughout the organization. It is important that you have programs in place that educate all personnel not only in these policies and procedures but why they exist, the rationale behind needing cyber security and its importance.

This also needs to apply to all levels of the organization.

This education should occur on an ongoing basis since the cyber threats you face and the cyber exposures that exist will continue to evolve as the predators create new was to disrupt your operations, new technologies arise, and you and your business partners change your business practices and procedures.

You also should consider having an internet accessible site that has your cyber security policies, procedures, and best practices available. You might also consider having a newsletter that updates all staff on new threats, practices and other cyber security considerations.

Sizing Considerations

There are serious considerations in how small, medium and large organizations address their cyber risks and exposures. The comments below are general guidelines and must be considered in light of your specific organizations structure and culture.

Small organizations

By definition you do not have extensive resources to devote to cyber threats and must rely on people wearing multiple hats. The good news is that many of the suggestions will be easy to implement since you will have fewer exposures and items to deal with. You also should not have major culture or communication issues since there are few of you and you are all in constant and close communication.

While each organization is different we suggest you focus on the simple easy tasks at first. For example making sure all default settings and passwords on your equipment are changed. Also make sure all people in your organization are made aware of the ways predators will try and compromise your organization. This may be done in a small organization by circulating articles and other publications.

Medium organizations

Your size puts you in a difficult situation. You likely have information and assets that the predators covet. Yet your resources are constrained.

This means our strategic segmentation approach may be your best bet. Your specific situation will determine what segments should have priority. As a first step we suggest a communication and education program be established, if possible piggybacked on existing programs, to make sure all in your organization are made aware of the risks that cyber threats pose and the security necessary to stop them.

Large organizations

Likely you have resources to address the issues involved so that means your biggest issues are likely to be in the culture and exposure areas since your size implies a great many access points and personnel with their own agendas.

While each organization is different we suggest you focus on the understanding your organizations culture and exposures as a parallel effort and make sure your existing cyber security personnel are part of the program. An education program that makes sure all in your organization are aware of the ways predators will try and compromise your organization. if such an education program is not already in existence one should be implemented as soon as possible. .

Links

Self-Assessments

Cyber Security Culture Barometer— a free self-assessment of the how supportive your organizations culture is towards cyber security

Videos

Cyber Exposure—A five minute video providing a quick overview of our strategy and approach.

Cyber Wack-a-Mole—A short video providing background on cyber wack-a-mole

Courses & Webinars

Understanding Cyber Exposure—A short course available through the Cyber Risk Academy providing background material for understanding cyber exposures.

Advanced Cyber Exposure Management Part 1—The first of a two part course that provides introduction to identifying cyber exposures.

Advanced Cyber Exposure Management Part 2—The second part of the course which provides information on how to manage cyber exposures will be available by year end.

Cyber Exposure Management—Why should you care? - This webinar will bring the following points to your attention: How Cyber exposures can hurt your organization in multiple ways; How Cyber exposures are not confined to purely technical areas; How If not addressed cyber threats will harm your organization

Publications

effective Cyber Exposure Management— Available on Amazon. An introduction to understanding, identifying and managing cyber exposure.

effective Enterprise Risk Management— Available on Amazon. A primer on effective enterprise risk management.

Standards

Example of widely accepted risk management standards are as follows. It should be noted that there are charges for many of their standards.

ISO (http://www.coso.org/guidance.htm) ISO 27001/27002 are the international standards for technical risk management principles and guidelines.

NIST Information Security Handbook: A Guide for Managers, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Personal Information:

Guides from the US Government of protecting personal information.

Protecting Personal Information: A Guide for Business, Federal Trade Commission, http://www.ftc.gov/infosecurity/

Privacy Policies: Say What You Mean and Mean What You Say, Federal Trade Commission, http://www.ftc.gov/bcp/edu/pubs/articles/art09.shtm

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.shtm

Information Compromise and the Risk of Identity Theft: Guidance for Your Business, Federal Trade Commission, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm

Cyber Threats

The following sites provide information regarding cyber threats.

CERT National Cyber Alert System, http://www.us-cert.gov/cas/signup.html

SANS Institute @RISK: The Consensus Security Alert, http://www.sans.org/newsletters/risk/?portal=6ea651380cdb76a250c69e382baf5c61

FBI's Internet Crime Complaint Center: http://www.ic3.gov/default.aspx

IBM's Cyber Security Intelligence Index: You have to fill out a form but the information covers the world and can be a great help.

https://www-03.ibm.com/security/data-breach/cyber-security-index.html

Threat Assessment

An Introduction to Computer Security: The NIST Handbook Chapters 14 and 18, National Institute of Standards and Technology,http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Common Sense Guide to Prevention and Detection of Insider Threats, United States Computer Emergency Readiness Team, http://www.us-cert.gov/reading_room/

An Introduction to Computer Security: The NIST Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

