

A photograph of several old, weathered keys of various shapes and sizes, including a large skeleton key and a smaller key with a circular head, resting on a dark, cracked wooden surface. The keys are arranged in a cluster, with some overlapping.

Cyber Security
*Combating the
Relentless Assault*

Cyber Security is:

- The comprehensive protection of information assets related to that business or company
- The defense against any unauthorized access or use of that information, and malicious or otherwise disruptive attacks to obtain or prevent access to or use of that information.

The growing number of Cyber Security threats, combined with the increasing complexity of those threats, have **finally** caught the attention of organization leaders.

Iron Key Group® Insight:

1. Our reliance on technology is so great...

The need to obtain and use information is so vital to businesses today, and growing on a daily basis. We are all vulnerable to technology problems, human error, lack of education and awareness, and casual and targeted attacks.

2. Today's threat landscape is real.

Targeted malware has become the norm, hacking techniques are becoming more numerous and complex, and the current technology environment – cloud, mobile, Big Data, Internet of Things – is making today's threat landscape something that can no longer be ignored.

3. Cyber Security is still a friction point in many organizations.

It is still largely viewed as a cost center. You must understand the risks to your organization, and ultimately align your IT your security strategy with corporate and IT strategies to ensure support and ongoing value.



<= PERCEIVED RISK

<= ACTUAL RISK

What Is The True Risk?

Do you understand the true risk of cyberthreats to your organization? Do you know what is lurking under the surface? Educating yourself and your company on the likely and probable threats and their associated risks is critical to reducing your overall risk posture.

90%

“90% all security incidents investigated recognize human error and lack of awareness as a contributing factor”

[IBM Security Services 2014 Cyber Security Intelligence Index](#)

How Real Is The Cyber Threat?



Likely Threats

Threat exists, probability is high:

- Hardware failures
- Human error or carelessness
- Disgruntled employee with the motive and the means to do harm
- Virus or malware outbreak
- Spam & phishing schemes
- Usually inexpensive and relatively easy to address

External attacks are usually random: people or cyberbots trolling the internet with the hope of finding a vulnerability to easily exploit, (i.e. “the front door or back window was unlocked and open”)

Unlikely Threats

Threat is high, probability is low:

- Full-scale information data breach/theft
- Usually expensive and more challenging to address

Usually targeted: large corporations with millions/ billions of records of information, such as credit card #'s, social security #'s, etc. (i.e. “the front door was locked and the alarm was on, but we picked the lock and hacked the code”)

- Ashley Madison, Home Depot, Staples, Target, Sony Pictures, Citigroup

How Real Is The Cyber Threat?



“We must ensure that public and private organizations, large and small, understand their Cyber Security risks and have the standards and technologies necessary to best protect themselves.”

NIST (National Institute of Standards and Technology) - 2016

FACT

Hackers and organized crime groups do perpetrate direct attacks, but they are not the most prevalent

FACT

Service providers, consultants and contractors are fast moving up the list, as they typically have unfettered access to both physical environments and computer systems

THE BIGGEST THREAT?

Current and former employees remain the biggest threat to a company's data and systems protection:

- **Current Employees:** Vulnerable due to weak passwords, phishing schemes, sending company info to personal accounts, lack of training & awareness
- **Former Employees:** Disgruntled employees taking company info on exit, exploiting credentials that were never removed

Cyber Security Measures To Protect Your Information and Technology Assets

There are a number of cybersecurity-related measures you can take to ensure you have a comprehensive strategy in place to protect your company's valuable information and technology assets. While not nearly complete, this is a good start:

- ✓ Security Awareness & Training
- ✓ Local Administrative Rights
- ✓ Spam Filter
- ✓ Anti-Virus
- ✓ Anti-Malware
- ✓ Firewall(s)
- ✓ Wireless Network Review
- ✓ Content Filtering
- ✓ Patches & Updates
- ✓ Data Backups & Restores
- ✓ Access Control
- ✓ Threat Assessment/Penetration Test
- ✓ Disaster Recovery/Business Continuity
- ✓ Intrusion Prevention
- ✓ Cybersecurity-Related Policies
- ✓ Cybersecurity Insurance

The following pages allow you to evaluate and score the status of your current security posture on the above measures. The legend to the left outlines the different statuses you can use for those measures:



Measure is currently in place and operating as expected







Measure is currently in place, but there are gaps that exist



Measure is not currently in place


Evaluate and Score Your Current Security Posture – How Do You Stack Up?



 Security Measure	Current Score/Status	
1. Security Awareness & Training Educate all employees that emails and attachments that are received from unknown sources should not be opened, and should be deleted immediately; ensure they understand the threats from visiting websites and their associated ads		(Sample score to the left requires detail on the evidence of the effective operating control)
2. Local Administrative Rights Review A review of all local desktop PCs and their respective accounts' rights has been reviewed within the last 12 months to ensure that all administrative rights have been revoked to limit the number of non-standard or non-authorized software or hardware installations		(Sample score to the left requires detail on the gaps that exist with the operating control)
3. Spam Filter Implement a spam filter that will detect unsolicited and unwanted email and prevent it from getting to users' inboxes. Outside of being annoying and unproductive, spam is yet another way for viruses and malware to be introduced into a company's technology environment		(Sample score to the left requires detail on why the measure is not in place)
4. Anti-Virus Implement a full-scale anti-virus tool that detects and cleans up existing virus threats.		


Evaluate and Score Your Current Security Posture – How Do You Stack Up (Cont.)?



 Security Measure	Current Status	
5. Anti-Malware Implement a full-scale anti-malware tool that detects and cleans up existing malware threats that would not be otherwise detected and cleaned by an anti-virus solution		
6. Firewall(s) Implement firewall protection. Firewalls are network appliances that are configured to accept allowable incoming traffic and block unknown or disallowed traffic to prevent outside attacks from infiltrating a company's network		
7. Wireless Network Review A review of the wireless network (if applicable) was performed in the last 12 months to ensure all wireless controllers and access points are utilizing best-practice security measures		
8. Content Filtering Implement content filtering technology that will scan the companies' web-browsing and file/content downloading activities for any malicious code or content		


Evaluate and Score Your Current Security Posture – How Do You Stack Up (Cont.)?



 Security Measure	Current Status	
9. Patches/Updates Ensure all servers and their operating systems and applications have the latest updates and security patches applied		
10. Data Backups & Restores Implement sound backup and restore procedures to cover individual file restores and company-wide data recovery in the event that an unexpected incident results in data loss		
11. Access Control Ensure that all network/Active Directory credentials are in place, and that passwords are complex (min. 8 characters with at least one capital letter, one number and one special character), and that they are forced to change a minimum of every 90 days		
12. Threat Assessment/Penetration Test Perform a detailed threat assessment of your environment, including an external network penetration test to ensure you understand what current risks and threats exist		
13. Disaster Recovery/Business Continuity Ensure that the company has a comprehensive DR/BCP plan in place, and that it is tested on a regular (i.e. yearly) basis		

Evaluate and Score Your Current Security Posture – How Do You Stack Up (Cont.)?



 Security Measure	Current Status	
14. Intrusion Detection/Prevention Implement a system that uses a preemptive approach to network security, and that is used to identify potential threats. With such a system, the ability exists to take immediate action based on a set of pre-determined rules that have been established		
15. Cyber Security- Related Policies Write and publish a set of cybersecurity-related policies that may include (but not be limited to): Acceptable Use, Access Control, Remote Access, Wireless Access, etc. Ensure that all company employees have read and understood the policies and that provisions are in place to handle non-compliance.		
16. Cyber Security Insurance Purchase an insurance policy designed to mitigate losses from a variety of Cyber Security incidents, including data breaches, business interruption, and network damage.		



NOTE: *Beyond the above measures listed, there are several other security measures that can be put in place for your firm's information and technology assets to be as protected as possible. Given the "moving target" nature of today's cyberthreats, Iron Key Group® cannot guarantee that implementing the above or any other security measures will prevent a Cyber Security incident/event from occurring.*

Information Security Is Essential To Protect Your Systems And Assets



Situation

Technology sophistication and business adoption, the propagation of hacking techniques, and the expansion of hacking motivations from financial to now social, political, or strategic motivations have resulted in organizations facing major security risk. Every organization needs some kind of information security program to protect their systems and assets. Organizations today face pressures from regulatory or legal obligations, customer requirements, and now senior management expectations.

Complication

Performing an accurate assessment of your current security operations and maturity levels can be extremely hard when you don't know what to assess or how, and don't understand the risks and threats to your business; not to mention an assessment alone is only the starting point. Senior management wants to know that adequate targets have been determined and there is a robust plan on how they are going to be met.

Resolution

Iron Key Group® has developed and tested a robust information security framework with supporting methodologies to generate your organization's comprehensive, highly actionable, and measurable security strategy and roadmap:

- ✓ Iron Key Group® best of breed security framework combines COBIT, ISACA, PCI, ISO and NIST security components to ensure all areas of security are considered and covered.
- ✓ Robust security requirements gathering across the organization, key stakeholders, customers, regulators, and other parties ensure the security strategy is built in alignment to and support of enterprise and IT strategies and plans.
- ✓ A comprehensive current state assessment, gap analysis, and initiative generation ensures nothing is left uncovered.
- ✓ Tested and proven rationalization and prioritization methodologies ensure the strategy you generate is not only the one the organization needs, but the one the organization will support.