GlobalRisk Community

Breaking Into Cyber Security

by Boris Agranovich

the founder of GlobalRisk Academy

In association with GlobalRisk Community:

The world's premier online risk management forum for professionals

Executive Summary

- Module 1 –What is Cyber Security and What Are the Basics
- Module 2 – Cyber Compliance in the Industrial Revolution
- Module 3 –How To Ensure a Balanced Cybersecurity Plan

Breaking Into Cyber Security

Module 1

What is Cyber Security and What Are the Basics

GlobalRisk Community

www.globalriskacademy.com

Introduction

The cyber risk landscape is evolving rapidly in a multitude of areas.

Governments are facing an unprecedented level of cyber attacks and threats with the potential to undermine national security and critical infrastructure, while businesses that store confidential customer and client information online are fighting to maintain their reputations in the wake of massive data breaches.

Introduction

The potential economic fallout from the cyber threat cannot be underestimated.

Economic thought leaders have warned of a digital disintegration, a scenario in which cyberspace could be completely undermined due to strengthening attacks where the Internet is no longer a trusted medium for communication or commerce, at a huge cost to economies and societies.

Cyber Security Attacks Are Increasing at a Rapid Rate

Cyber-attacks are now taking place throughout the world at an accelerating pace.

Recently, the Office of Personnel Management announced that hackers stole social security numbers and other highly sensitive information for more than 21 million people. Sony Pictures had their company and personal emails hacked as well as salary information for the vice presidents and executives. Stuxnet is a rumored US and Israeli computer virus designed to attack the centrifuges used to control machinery critical for the manufacture of nuclear weapons.

Cyber Security Attacks Are Increasing at a Rapid Rate

As more corporations and governments have come to rely on the internet, this has left them susceptible to malicious cyber-attacks from hacker groups and nation states that employ hackers to infiltrate countries sensitive computer systems.

There is a dire need for cyber security professionals to fill the many white collar openings that are popping up as companies struggle to protect their programs from outside attacks.

GlobalRisk Community

How to Become a Cyber Security Specialist

You have been reading the news about all the recent cyber-attacks, you have an interest in computers and you want to embark on a new career as a cyber security professional. Where do you start? There are 3 major paths you can take to further your career in information technology and information security:

- Take and Pass Cybersecurity Certifications
- Obtain a Cybersecurity Degree from an Accredited University
- Start by taking this course “Breaking Into Cyber Security” to understand the Cyber Security landscape and develop a career development plan for yourself

GlobalRisk Community

Recent Cyber Attacks

Victims of recent attacks include such well-known brands as

- eBay,
- Target,
- Neiman Marcus,
- Michaels Stores,
- NATO,
- JPMorgan Chase,
- Adobe,
- Living Social. The list goes on.

What is Cyber Security?

Cyber Security is an information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

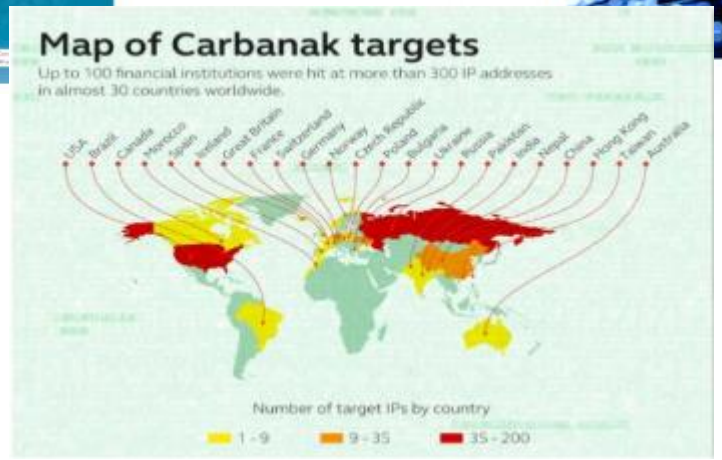
Cybersecurity impacts all of us when we go online, use our mobile device or tablet, or use a cloud-based service. We all interact with various tools designed to protect your personal information, similar to tools used to protect our nation's infrastructure. It is critical for everyone to understand cybersecurity and our role in being safe while staying connected to minimize the chance of an incident.

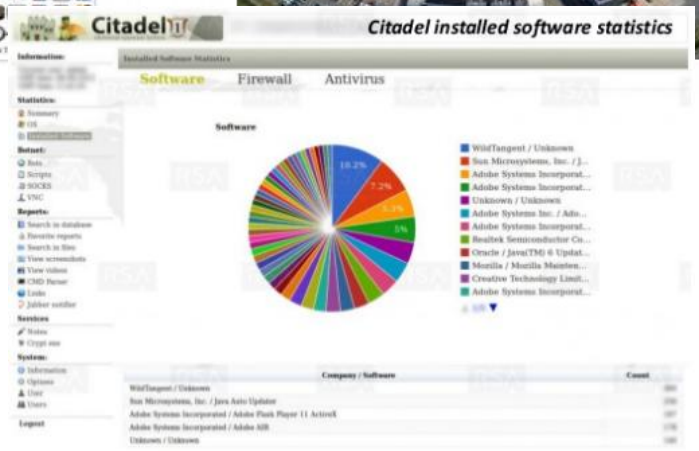
What is Cyber Security?

Cybersecurity can be defined as: “The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”

Cybersecurity focuses on protecting computers, mobile devices, tablets, networks, programs and data from unauthorized access or manipulation. Understanding cybersecurity is the first step to protecting yourself, your family and your organization.

Cyber Threats Are a Real Danger! Governments are Worried





GlobalRisk Community

www.globalriskacademy.com

Cyber Threats Are a Real Danger

In a world where cyber threats are a constant danger, companies find themselves in an ongoing battle to keep their data safe. A plethora of risks now exist as cyber-criminals continually seek new ways to breach our borders and get their hands on our vital information.

However, did you know that 99.9% of exploits are possible because organizations don't address basic security hygiene? The fact is that a lot of industries focus on the wrong things, often using security strategies that are fundamentally flawed and ultimately do not provide the right sort of protection they need.

GlobalRisk Community

Cyber Security Vocabulary

As you master new cybersecurity skills, you'll be exposed to new terms that are constantly growing and evolving. Each new challenge and achievement will open the doors to new concepts that must be both clearly defined and proficiently demonstrated.

While some computer security terms have become rather commonplace in our society, others remain a bit mysterious to those encountering them for the first time.

Here are some basic Internet and cybersecurity terms that may help you as you increase your knowledge in this challenging field.

Cyber Security Vocabulary

- ***Antivirus Software.*** Most Internet users are well aware of these programs since nearly every computer sold today provides at least short – term access to this type of software. In a nutshell, these programs protect your computer from Internet viruses or codes that can quickly disable your computer (or an entire network). When functioning properly with all necessary updates, this software will constantly monitor your computer to prevent viruses from "infecting" it;
- ***Attacks.*** People stage intentional active and passive attacks while trying to bypass computer security controls. During an ***active attack***, the perpetrator tries to alter a system's data, resources or operations. However, a ***passive attack*** simply involves trying to access and use a computer system's information –*without* trying to alter its resources, operations or data;

Cyber Security Vocabulary

- ***Back Door.*** Sometimes used interchangeably with the term “trap door,” a software or hardware designer makes ones of these to allow herself (or privileged others) to circumvent computer security;
- ***Blended Threats.*** Hackers or cyber terrorists who approach computer networks using blended threats are trying to maximize the damage they can inflict by using different traits of both ***viruses*** and ***worms***. For example, an attacker might try to send out an e-mail virus with a Trojan horse embedded in an HTML file. Past examples of blended threats include both Bugbear and CodeRed;

Cyber Security Vocabulary

- ***Bots.*** A person attacks your computer with a bot – or remote control agent – by bypassing your firewall and antivirus software. Once installed on your computer, a bot becomes part of a bot network (***botnet***) that the hacker or ***bot owner/bot herder*** can then manipulate at will. Bots can install various types of ***spyware*** (or malicious logic) on your computer, allowing the bot owner to take it over whenever it's connected to the Internet. Some people use the term ***"zombie"*** interchangeably with the term "bot;"
- ***Cybersecurity.*** "The activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation;"

GlobalRisk Community

Cyber Security Vocabulary

- ***Cyber Exercise.*** "This is a planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption;"
- ***Encryption.*** "The process of translating plaintext into ciphertext." Unencrypted data is called ***plaintext*** while encrypted data is referred to as ***ciphertext***. The two main types of encryption are referred to as asymmetric and symmetric;

Cyber Security Vocabulary

- ***Firewall.*** "A capability to limit network traffic between networks and/or information systems." In other words, it's "A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized;"
- ***A Gateway.*** This is simply a bridge between two computer networks;
- ***Hacker.*** An unauthorized user who seeks to maliciously disrupt or permanently damage an individual computer – or entire network of computers;

GlobalRisk Community

Cyber Security Vocabulary

- ***Internet.*** A constantly growing number of computer users regularly communicate with each other via this worldwide global network. In fact, there were 3.5 billion Internet users as of the beginning of 2016*;
- ***Intranet.*** "A network based on TCP/ICP protocols (an internet) belonging to an organization, usually a corporation, accessible only to the organization's members, employees, or others with authorization." A special firewall is designed to protect an intranet website from those unauthorized to use it;

*www.statista.com

GlobalRisk Community

Cyber Security Vocabulary

- ***A Keylogger.*** This type of harmful or malicious program is used to infiltrate your computer to record information about all of your computer keyboard activities, including all Internet browsing activities, e-mail usage and instant messaging communications;
- ***Malicious Code.*** This refers to any type of software that's installed in your computer (system) and can perform unauthorized activities. **Malware** is a similar term that refers to malicious software created to damage, disrupt or even possibly destroy a computer (system) with viruses, Trojan horses and other harmful programs;

Cyber Security Vocabulary

- ***Phishing.*** These Internet scam programs often contact unsuspecting people via e-mail, urging them to visit *fake* websites designed to look like those run by well-known banks or other financial institutions. Perpetrators then try to obtain private information by telling users it's time to update their account passwords or usernames. If unwitting people comply, all types of fraud, including identity theft, may result;
- ***Spyware.*** This type of software is installed on a network of computers without the owner's knowledge. Its main purpose is to gather personal/group information and communicate it to an unknown third party. Spyware can monitor your activities and even pick up critical information like credit card numbers, usernames and passwords;

Cyber Security Vocabulary

- ***Trojan Horse.*** This type of harmful computer program can be easily installed on your computer while you're downloading unknown programs or files off the Internet (or simply opening up unfamiliar email attachments). A Trojan horse will nearly always damage your computer in some way;
- ***Virus.*** A computer virus is harmful "software" that attaches itself to other programs in order to impair or destroy a computer's ability to function normally;
- ***Worm.*** This is an independent program that replicates (reproduces) from machine to machine across network connections, often clogging networks and information systems as it spreads.

Cyber Security Best Practices

There are, of course, a lot of best practices out there, but how do you bring those frameworks to life within your organization?

In this training, we will explore some of the main threats companies face, evaluate the effect of the industrial revolution, and discuss the ways in which organizations can address the 5 key components of cyber risk framework with confidence to ensure a better overall security posture.

Breaking Into Cyber Security

Module 2

Cyber Compliance in the Industrial Revolution

GlobalRisk Community

www.globalriskacademy.com

4th Industrial Revolution— Complexity Increases Over Time

1784
Steam engine

1870
Mass production

1969
Information technology

2020
Cyber-physical systems

GlobalRisk Community

www.globalriskacademy.com

The Path to Cyber Resilience

Cyber breaches happen. That is the new reality. However, with cyber resilience, organizations can respond with agility to cyberattacks.

So, despite an attack, the organization carries on— patients are treated, power is generated, commerce flows.

The Path to Cyber Resilience

This new approach emphasizes five fundamental steps:

1. Identify your most critical assets—What do you have that is most valuable to others?

2. Gather intelligence on cyber threats—Who are the bad actors?

3. Understand your digital profile—What does your online activity signal to others?

4. Build a resilient system—What are the most critical elements of defense?

5. Plan for a breach—What can you do now to prepare for a crisis?

Identify Your Most Critical Assets

All data is not created equal. Yet, the traditional approach to cyber defense is to construct a perimeter and treat all assets in a similar fashion. This method can lead to inefficiencies and misalignment of resources.

A better approach begins with a simple question: Why should my organization be concerned about cybersecurity?

Answering this question with precision requires identifying which data, applications, and systems are essential for your organization to conduct operations, and then developing a cyber strategy that is driven by protecting core business functions—and not merely responding to threats.

GlobalRisk Community

Identify Your Most Critical Assets

So, what do you have to lose? What are your most critical assets? Intellectual property?

Turbines? Customer data? Medical histories? Trade secrets? Proprietary financial data?

Industrial control systems?

Gather Intelligence On Cyber Threats

Evolution in the nature and sophistication of cyber threats has been stunning. And, it is only beginning.

In just the past few years, hackers have grown far more sophisticated, their attacks more complex, targets more encompassing, and the impact of those attacks more damaging.

There is now a highly advanced underground online economy where hacker tools and illicitly obtained data are readily available. Companies must now confront the specter of data manipulation, extortion, and potential acts of terrorism. Understanding the ever-changing threat landscape plays an essential role in cyber resiliency.

GlobalRisk Community

Gather Intelligence On Cyber Threats

The cyber-threat landscape

Two other factors accentuate the threat posed by cyberattacks. First, on average, it takes an organization more than 146 days to realize that its systems have been breached. Indeed, in multiple instances, breaches have been undetected for years.

Second, in more than 65 percent of cyberattacks, it is a third party, and not the organization itself, which discovers that a breach occurred. For an organization to adopt cyber resilience, mature cyber threat intelligence is essential to identify threats and reduce the period of exposure.

Gather Intelligence On Cyber Threats

Attacks on physical assets and critical infrastructure

Over the past several years, most publicly reported breaches have concerned data theft—such as credit cards, Social Security numbers, and patient records. Attacks are now morphing into the realm of physical assets that threaten the critical infrastructure—including electric grids, transportation systems, satellites, civilian nuclear facilities, and telecommunications networks.

By exploiting industrial control systems and critical infrastructure, cyberattacks now pose a threat to public safety and economic security.

Gather Intelligence On Cyber Threats

There is technology that can identify a series of advanced threat actors who possess a high-cyber capability to conduct network attacks and use a range of tactics and target critical industries worldwide.

Recent threats to operational technology included:

- A new type of malware, which creates a “loop” that sends instructions to hardware to alter its operations while appearing, on the surface, to be working properly.
- A malware discovered by Norwegian law enforcement in 2014 that compromised 50 Norwegian energy companies.
- The leaking of partial blueprints of a South Korean nuclear reactor by hacktivists linked to state actors.

GlobalRisk Community

Understand Your Digital Profile

Big Data approach to analyzing cyber risk—the “outside-in” perspective

Hackers look for opportunity and probe for weakness—a combination of the value of your assets and vulnerability of your systems. Big Data can now be harnessed to assess the likely motivation for and potential susceptibility to cyber events by relying exclusively on data points beyond an organization’s perimeter. This is the outside-in approach.

In the digital era, each organization creates a footprint through its online activity. Your business, just like an individual, leaves a trail of digital breadcrumbs behind.

Understand Your Digital Profile

For example, do your servers share web hosting platforms with others, or worse, with highly targeted companies?

Can hackers spot instances of unpatched software by monitoring browsers used by employees to access the Internet?

Is your organization subject to activity on the so-called “dark web?”

What do your job postings for IT positions reveal about your operations?

Will poor employee morale, as reflected in external surveys, correlate to insider attacks?

What is your web presence and how strong is it?

GlobalRisk Community

Six Core Elements of Cyber Security

Cybersecurity strategy

Cybersecurity strategy is the function that defines the enterprise approach within the context of an organization's overall business objectives and activities.

Governance risk & compliance

Management of cybersecurity risks and capability alongside the business and regulatory environment.

Security operations

Situational awareness alongside the ability to monitor, manage, and respond to cyber threats.

Security assets & infrastructure

Cybersecurity-specific controls and services that enable a resilient digital infrastructure.

3rd party & cloud security

Evaluation and integration of risks associated with cloud and third-party providers of services.

Cybersecurity culture & awareness

A posture of preparedness and proactive response: balancing focus on people, process, and tools to help get ahead of cybercrime.

GlobalRisk Community

Build a Resilient System

With a deeper understanding of your critical assets and overall threat environment, the next step is to develop a strategic framework for deploying your resources. This process should address six core elements:

1. Cybersecurity strategy
2. Governance, risk, and compliance
3. Security operations
4. Security assets and infrastructure
5. Third party and cloud security
6. Cybersecurity culture and awareness

Build a Resilient System

1. Cybersecurity strategy

An organization's overarching strategy determines its risk management goals. Objectives may be as basic as safeguarding data and ensuring confidentiality, integrity, and availability or improving security by reducing vulnerabilities. More complex priorities include benchmarking progress against an established industry standard.

Build a Resilient System

1. Cybersecurity strategy

Challenge: Stove-piping

Poor communication, lack of management engagement, and an absence of board oversight are barriers to effective development of a cyber strategy. Cyber-risk management is an enterprise concern, not simply a technology issue.

However, even organizations that accept this notion can struggle to embrace sound enterprise risk management practices unless senior management takes ownership of this issue, and the board provides necessary oversight.

GlobalRisk Community

Build a Resilient System

2. Governance, risk, and compliance

Almost more than any other risk a company faces, are the myriad of stakeholders involved in building cyber resilience. The board of directors. Multiple members of the senior management team, including the CEO, CFO, general counsel, CIO, head of HR, and chief information security officer (CISO). Your employees. Your vendors.

The role of the board and each member of senior management, in particular, should be clearly articulated in order to enhance your organization's agility to respond to a dynamic threat and avoid conflict.

Build a Resilient System

2. Governance, risk, and compliance

Challenge: An avalanche of new laws

Cybersecurity laws, regulations, and policies are fragmented and in a constant state of flux. It is estimated that more than 140 new pieces of security or privacy legislation will be passed globally in the next two years.

There is almost no commonly accepted framework that an enterprise can use across industry, and national and regional environments. Organizations must strive to adopt enterprise standards and protocols to guide the appropriate allocation of resources.

Build a Resilient System

3. Security operations

A company's security operations identify threats to the organization and direct real-time responses to mitigate damage and business disruption. A key responsibility of security operations is to implement tactical controls that keep pace with evolving threats.

For example, as social engineering attacks like spear phishing prove to be distressingly effective, detonation or "sandbox" software may mitigate this risk. As organizations struggle to protect personally identifiable information, data loss prevention (DLP) software is an important component of an organization's security toolkit.

Build a Resilient System

3. Security operations

Challenge: Attribution

The inability of companies to identify the sources of attacks provides hackers with a significant advantage. Advanced attackers acting with impunity rapidly change tactics to bypass traditional defenses.

Industry and government leaders must accelerate their commitment to gathering and sharing threat intelligence to improve attribution.

Build a Resilient System

4. Security assets and infrastructure

These include data centers, servers, software, and personal devices, which should employ controls that protect data, users, applications, and networks from threats.

Legacy systems create inherent vulnerabilities for many reasons, including the challenge of patching known software vulnerabilities.

Build a Resilient System

4. Security assets and infrastructure

Challenge: Shrinking the attack surface

The rapid development of the Internet of Things and proliferation of mobile devices create an ever-expanding set of entry points for hackers. For many organizations, data sprawl is the top cyber vulnerability.

To shrink your attack surface, your organization should review its network architectures to eliminate unneeded Internet connections and avoid accumulating data for no reason. Limiting your attackers' opportunities is as important as any investment in technology.

Build a Resilient System

5. Third party and cloud security

A key lesson of prominent data breaches over the past two years is that any organization is only as cyber resilient as the weakest of its third-party vendors. Regulators, focused on third-party vulnerabilities, are introducing cybersecurity mandates related to vendors.

An organization must now actively manage its network supply chain ecosystem, and align controls with the vendor's network activities. At the same time, moving data and applications to the cloud—with the right safeguards—can increase security and resilience.

Build a Resilient System

5. Third party and cloud security

Challenge: Assessment of cloud performance

While outsourcing offers great advantages and, at times, improved security, it also adds complexity. Organizations should establish controls that:

- Limit vendor access within your network.

- Avoid overreliance on any specific outsourced vendor.

- Impose an obligation on vendors to provide notice before transferring your data to other jurisdictions.

GlobalRisk Community

Build a Resilient System

6. Cybersecurity culture and awareness

Evolving culture to meet threats—Technology solutions, including end-to-end encryption, cannot eliminate cyber risk. More than 90 percent of successful cyberattacks are launched via spear phishing campaigns. Accordingly, creating a cyber-aware culture and providing training for employees are critical elements of cyber resilience.

Many, if not most, cyber breaches trace back to human error. Accordingly, organizations must focus on their people and processes for addressing cyber risk. Cyber resilience must reside in the organization's DNA, so it becomes an organizational imperative to protect and enable digital interactions

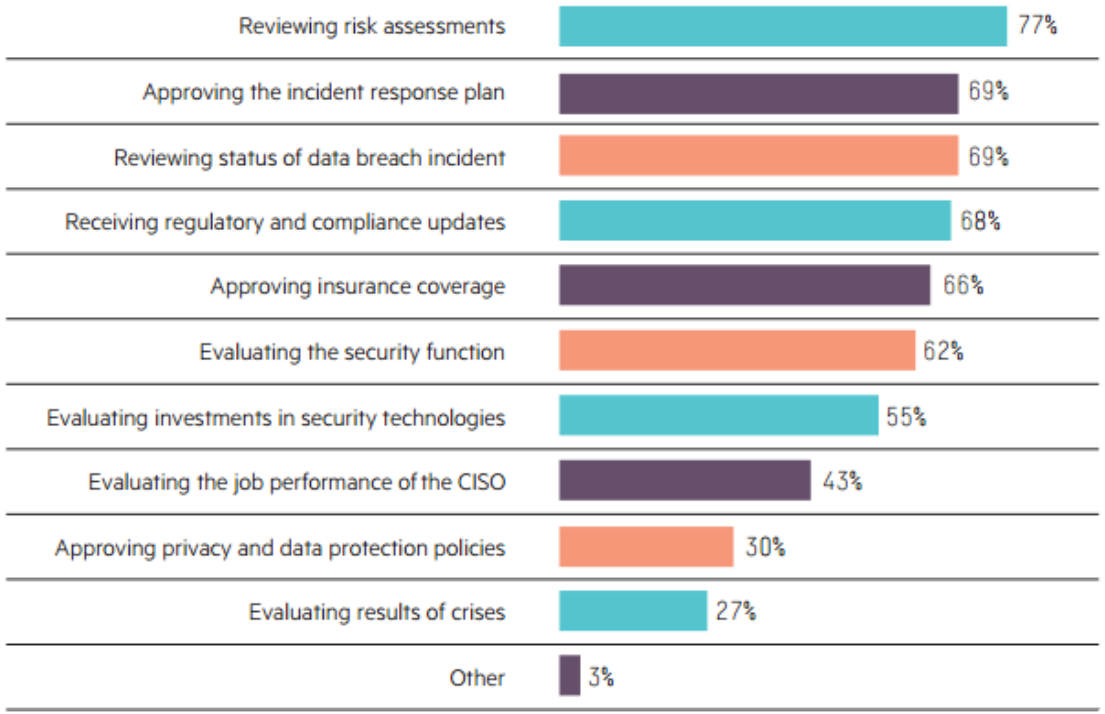
Build a Resilient System

6. Cybersecurity culture and awareness

Challenge: Challenge: Lack of focus on the user

Training should never grow stale or formulaic. Employees can be an organization's greatest vulnerability. A key challenge is to convert this vulnerability into an asset by training employees to become the first responders—who recognize incidents and protect the organization.

Role of Senior Executives in Incident Response*



*The Importance of Senior Executive Involvement in Breach Response, Ponemon Institute LLC, sponsored by HPE Security Service, October 2014

GlobalRisk Community

www.globalriskacademy.com

Plan for a Breach

- Cyber resilience through response and recovery

Almost inevitably, an organization's efforts to prevent attacks will eventually fail. Cyber resilience depends on an organization's ability to respond to a significant breach and continue operating effectively.

In this regard, there are two important steps to consider: contingency planning and the mitigation and transfer of financial risk.

Plan for a Breach

Contingency planning

Operating on the premise that every institution will ultimately be breached, contingency planning is critical. For example:

- Does your organization have a written incident response plan?
- Which executive will lead your incident response?
- Have you engaged in a simulated exercise to test your plan?
- Which outside advisors will you depend on? Have you engaged them on retainer?
- Have you developed relationships with key government officials?

GlobalRisk Community

Breaking Into Cyber Security

Module 3

How To Ensure a Balanced Cybersecurity Plan

GlobalRisk Community

www.globalriskacademy.com

Balanced Cybersecurity Plan

Risk professionals have grown more aware of the impact that the disclosure of personal data — whether through an employee error or a cyber-attack — can do to their businesses.

But cyber risk is broad, and many companies may not be preparing for non-privacy cyber incidents — which could be the biggest threats to their organizations.

Media Focuses on Privacy

Historically, businesses have considered network security breaches and loss of personal information to be synonymous with the term “cyber risk.” That’s largely because of the significant media attention given to data breaches, primarily in the US where breach notification laws are rigorous.

For some businesses — for example, retailers, health care organizations, and higher education — privacy risk may well be the biggest concern.

But for others — including manufacturers, energy companies, and other industrial organizations — disruption is a significant risk.

Align Cyber Risks to Risk Profile

Understanding your organization's cybersecurity profile is critical to managing risk effectively. To manage the cyber risk that can undermine your core operations, your organization should take the following three steps:

- Perform an enterprise-wide cyber risk assessment that defines the assets you have at risk.
- Develop a strategy for preventing the potential compromise of those assets.
- Build a plan to respond to an attack on those assets.

GlobalRisk Community

Align Cyber Risks to Risk Profile

Completing these actions can help you build a framework for understanding your unique cyber risks and the ways you can respond to them. That will likely include purchasing insurance coverage.

The good news for businesses is that insurance — particularly cyber insurance coverage — is designed to respond to a variety of threats, including data breaches, cyber-related business interruption, cyber-crime, and data or software damage.

A Framework for Managing Cyber Risk

Truly effective cybersecurity will require that organizations are able to capably and quickly identify, mitigate, and manage cyber risks.

In addition, managers should identify cyber business risks by thoroughly scanning and analyzing all known and relevant risk factors, including those that may not be likely to occur. These risks should provide a starting point for establishing an effective cyber-risk management framework.

A Framework for Managing Cyber Risk

Simplified Cyber Risk Management Framework

GlobalRisk Community

Managing Cyber Risk Across the Enterprise

Making cyber risk a corporate risk management issue means engaging areas across the enterprise, including:

- Finance.
- Legal.
- Compliance.
- Operations.
- Board.
- HR.
- IT.

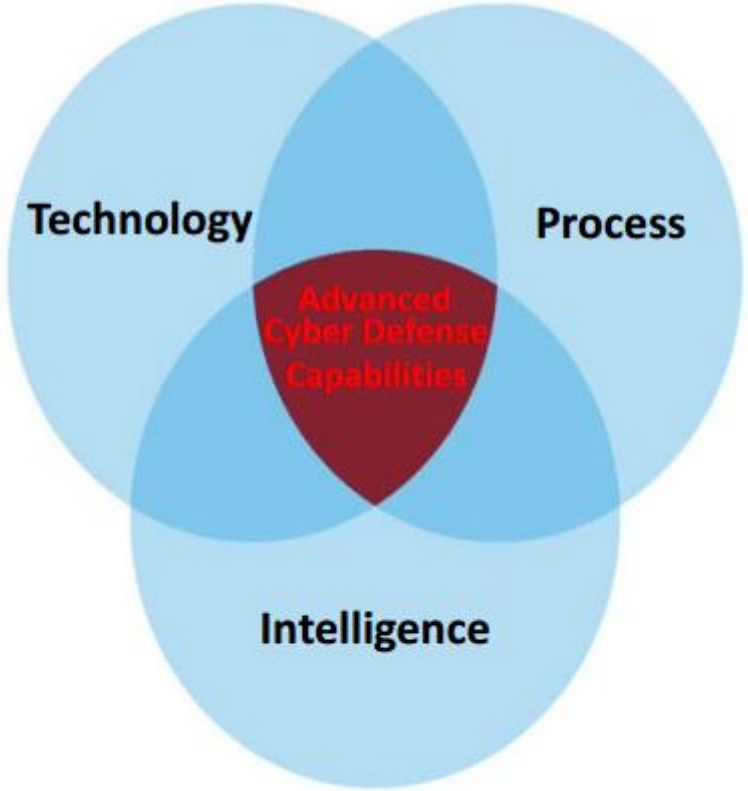
Four Rules For Managing Regulatory Analysis

1. Don’t leave cyber risk to just the IT department.
2. Look beyond attack prevention.
3. Connect your plans to external stakeholders and resources.
4. Include risk transfer as part of the approach.

GlobalRisk Community

Effective Cyber Defense

Minimize organizational risk and allow business to function while under continuous attack.



GlobalRisk Community

www.globalriskacademy.com

Effective Cyber Defense

• Predictive — Continuously measure enterprise attack surface and model potential threat vectors targeted at critical assets and data.

• Proactive — Hunt for intrusions. Discover and remediate / compensate for vulnerabilities.

• Responsive — Rapid analysis and containment of threats.

The 5 Key Components of Cyber Risk Framework

1. Protect valuable data

Organizations should identify their most valuable information assets, where these assets are located at any given time, and who has access to them.

The 5 Key Components of Cyber Risk Framework

2. Monitor for cyber risks

Traditional security monitoring approaches typically identify and react to cyber threats in isolation. Security tools are designed to identify specific unusual patterns or traffic types, and then alert operational teams to anomalous activity.

Effective cyber-risk monitoring, on the other hand, focuses on building a sustainable and resilient approach to assess intelligence inputs from various functional teams and to correlate and dynamically adjust in real time the organization's risk posture.

GlobalRisk Community

The 5 Key Components of Cyber Risk Framework

3. Understand your “cyber perimeter”

Today, a financial institution’s cyber perimeter extends to locations where data is stored, transmitted, and accessed—by internal employees and trusted partners.

Organizations should ensure they have transparency into this expanded cybersecurity perimeter, because any weakness in the perimeter can become a security vulnerability.

GlobalRisk Community

The 5 Key Components of Cyber Risk Framework

4. Improve cyber intelligence

Most financial institutions' threat-analysis efforts are scattered across several functions, physical locations, and systems. This disjointed nature and lack of a common methodology to leverage intelligence can be a significant barrier to robust cyber-risk intelligence.

To close the gap, organizations should establish a robust threat-analysis capability that is built on shared intelligence, data, and research from internal and external sources.

The 5 Key Components of Cyber Risk Framework

5. Report and take action

A strong governing team with the right knowledge, expertise, and influence will be necessary to advance cybersecurity.

An effective team can help ensure that monitoring systems are fluid and capable of precisely responding to cyber threats, and can empower management to appropriately react.

GlobalRisk Community

Security Operations Challenges

GlobalRisk Community

www.globalriskacademy.com

What's Ahead

2016 and beyond…

- More destructive attacks
- Attribution will be more important
- Counter-forensics will improve
- More threat actors will emerge
- More government involvement
- A return to standards for nonregulated industries
- More reliance on the cloud
- Cyber security will continue to be a board issue

GlobalRisk Community

Conclusion

Cyber risk is a race without a finish line. We hope this course helped connect the dots on some of the essential elements of this problematic issue, as well as increased understanding on how to approach this significant and persistent threat.

An effective cyber risk management program must be enterprise-wide, involving not only IT but also finance, legal, compliance, operations, and other departments.

Conclusion

We hope this training helped you to get a general understanding about Cyber Security.

Now you can in-depth your knowledge by taking the course

Understanding Cyber Exposure

or

Advanced Cyber Exposure Management - Identifying Cyber Exposures

or getting a cybersecurity degree at University. Doing both will give you a leg up on the competition and let you land that dream job in the fastest growing occupation in the world.

GlobalRisk Community

Did You Enjoy This Course?

Check out other courses in GlobalRisk Academy

Advance your career by joining an exclusive group of experts, interacting and building relations with risk professionals and service providers through a range of multimedia tools.

Are you ready for a Knowledge Boost?

"The best risk management and educational investment ever. I have learned about where Risk Management is going, been exposed to the best minds in the business, been challenged to rethink my assumptions about the Cyber Security, and gotten ideas about how to merge old and new systems."

—GRC Member Andrew Jones

Sign Up for a New Course

GlobalRisk Community

www.globalriskacademy.com

What Courses Does GlobalRisk Academy Offer?

Increase your professional knowledge and solve your business challenges by taking our practical, hands-on courses. **New trainings are added regularly!**

We are delighted to offer YOU, as our current student a **25% discount** on our excising courses and trainings.

You will have access to the latest information you need to stay ahead in your field.

Learn anytime, anywhere!

Follow the links on the next slide to benefit from this exclusive offer!

Start learning now!

GlobalRisk Community

www.globalriskacademy.com

GlobalRisk Academy Trainings and Courses

25% discount!

Mastering Operational Risk Within Financial Services

- http://globalriskacademy.com/courses/orm?product_id=28955&coupon_code=STUDENT

Understanding Cyber Exposure

- http://globalriskacademy.com/courses/cyber-exposure?product_id=34298&coupon_code=STUDENT

Profitable Trading Strategies Using Candlestick Charting

- http://globalriskacademy.com/courses/investment-strategies-using-candelstick-charting?product_id=21128&coupon_code=STUDENT

The Fundamentals of Credit Analytics

- http://globalriskacademy.com/courses/credit-analytics?product_id=25089&coupon_code=STUDENT

Creating Your Own Profitable Online Business Platform

- http://globalriskacademy.com/courses/create-your-own-online-business-platform?product_id=9990&coupon_code=STUDENT

GlobalRisk Community

www.globalriskacademy.com

GlobalRisk Academy Trainings and Courses

25% discount!

Finding Money To Start A Business in the United States

- http://globalriskacademy.com/courses/finding-money-for-starting-a-business?product_id=20705&coupon_code=STUDENT

Lean Shop Floor Training

- http://globalriskacademy.com/courses/lean-shop-floor-training-for-beginners?product_id=13656&coupon_code=STUDENT

Creating A Loan Package

- http://globalriskacademy.com/courses/lean-shop-floor-training-for-beginners?product_id=13656&coupon_code=STUDENT

Lean Bronze Certification Training

- http://globalriskacademy.com/courses/lean-bronze-certification-training?product_id=14050&coupon_code=STUDENT

Lean Leader Training

- http://globalriskacademy.com/courses/lean-leader-training-for-team-leads-and-supervisors?product_id=14069&coupon_code=STUDENT

GlobalRisk Community

www.globalriskacademy.com

Connect with **GlobalRisk Community**

and follow our feeds with articles, resources, blog posts, and other content to help you be a smarter professional in Financial, Banking, HR, IT, Cyber Security or other business sectors

GlobalRisk Community Forum
http://globalriskcommunity.com/forum

Boris Agranovich on Twitter
https://twitter.com/agranovb

Boris Agranovich on LinkedIn
https://www.linkedin.com/in/borisagranovich

GlobalRisk Community on Facebook
https://www.facebook.com/GlobalRiskCommunity

GlobalRisk Community

Do You Want to Become a Member of GlobalRisk Community?

JOIN US TODAY! »

Join over 20,000 happy members now to share knowledge, get new business, new contacts, jobs, latest research and exchange ideas.

Connections can change everything!

"Looks like a great site, very rich in content and very varied in media options for the content. I look forward to being a very regular visitor."

—GRC Member Marcus Cree, USA

GlobalRisk Community is the world's premier online risk management forum for professionals.

Risk Management best practices, risk education, resources, guides, insights, peer networking for Risk Professionals in financial, banking, HR, IT, Cyber Security and other businesses.

GlobalRisk Community

www.globalriskacademy.com