hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

HFMA/NEHIA
2022 Compliance & Internal Audit Conference

Wednesday, November 30 – Friday, December 2, 2022
Mystic Marriott Hotel, Groton, CT

Cybersecurity Risks - An Ever-Changing Concern For All!

Annual Compliance and Internal Audit Conference

NOVEMBER 30, 2022

Cyber Risk Service Provider

Director, IT Risk & Assurance
☎ 617.761.0722
✉ rgandy@cbiz.com

Ray Gandy, GCCC, MBA

- Leader of the New England IT Risk Practice
  - Outsourced/Co-Sourced Information Security Services
  - Cybersecurity Assessments & Prioritized Security Projects
- 30+ years of information technology experience
  - *Global IT Audit Director*
  - *CIO*
  - *Director, Infrastructure & Security*

Professional Memberships & Certifications

- GIAC Critical Controls Certification (GCCC)
- Vice President of ISACA Rhode Island Board
- AICPA, ISSA, SANS Institute
- AEFCU Board of Directors since 1995, Chairman
- Educause and REN-ISAC member

GENERAL DYNAMICS

Raytheon

United Technologies

Agenda

Cybersecurity Statistics & Trends

Regulatory Response

Supply Chain Attacks

Vendor Management

Security Controls Frameworks

Cybersecurity Posture Checklist

Cybersecurity Statistics & Trends

Threats, risks and technological advances in cybercrime are rising and increasing the costs and impacts to our businesses

The remote/hybrid workforce is here to stay

The operational reaction and financial impacts have created a strain on IT departments and information security efforts

No business/vertical is immune

Cybersecurity Statistics & Trends

Data on individuals is being analyzed, quantified, processed, stored, and sold on a colossal scale

Information/system access is more accessible to the standard employee than ever before

Companies are increasingly transitioning to digital/cloud-based work, systems, and records while engaging with other digital third parties

Bad actors are constantly finding creative new ways to access information and do the most harm

What Does a Hacker Look Like?

Cybersecurity Statistics & Trends

80% of firms have seen an increase in cyber attacks this year

Ransomware attacks rose 148% in March and the average ransomware payment rose 33% to $111,605 compared to Q4 2019

Malicious domains have spiked – information seekers beware

Embedded malware where you least expect it

Ransomware-as-a-service – a new (illegal) business model

Data Aggregators = Your Data for Sale

Cybersecurity Statistics & Trends

The average total cost of a data breach - **$3.86 million** - IBM

36 billion records exposed - RiskBasedSecurity

The average length of time to identify and contain a breach - **280 days** - IBM

World-wide spending on Cybersecurity expected to reach **$133.7 billion** in 2022 - Gartner

Technological Trends Impacting Cyber Risk

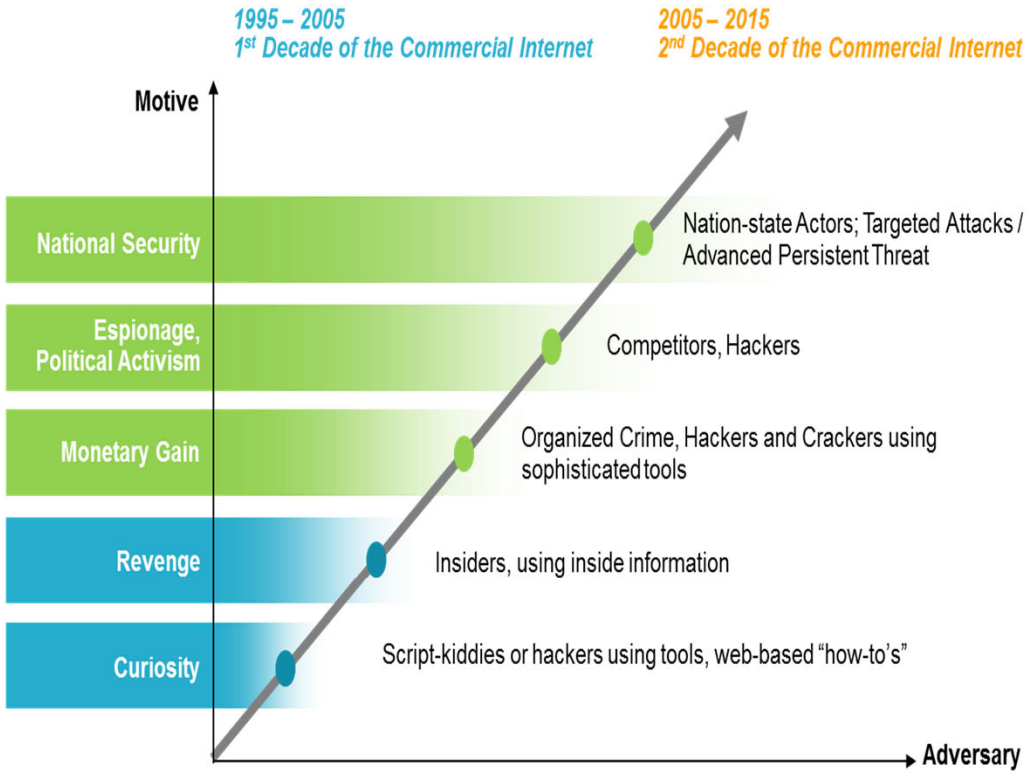
Key technologies expected to affect cybersecurity:

- Cloud vendor management
- Endpoint detection and response
- Multi-factor authentication and single sign-on
- Preservation of data authenticity and integrity
- Security of intellectual property
- Employee and client data privacy and governance

Data breach costs rose from $3.86M to $4.24M

- The highest average total cost in the 17-year history of this report *(Ponemon Report)*

Cyber Security Threats / Actors are Increasing



Source: Verizon Data Breach Report

Services Are Readily Available On the Dark Web

DDoS-As-A-Service Popular on the Darknet

By **Richard** - April 12, 2017

Attackers on the darknet are turning a handsome profit by offering DDoS-for-hire services according to Kaspersky Lab.

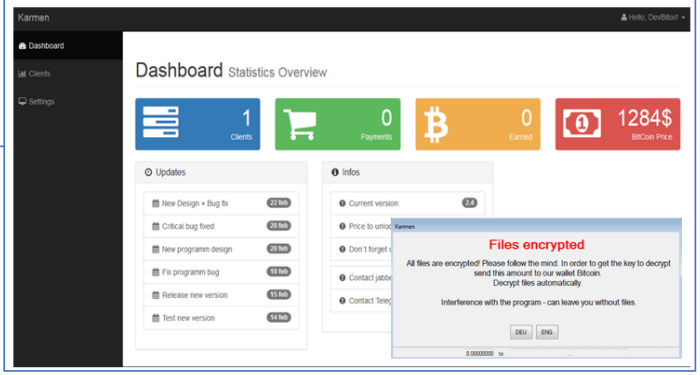
Kaspersky says that these cybercriminals enjoy profit margins of up to 95% solely by offering DDoS services on the darknet.

Kaspersky Lab reveals that cyber criminal making up to a 95% profit by offering DD service on the dark web.

The Hacker News™
Security in a serious way

Russian Hacker Selling Cheap Ransomware-as-a-Service On Dark Web

Tuesday, April 18, 2017 Swati Khandelwal



Internal Threats Are Just as Real

Types of insider threats according to Verizon

Malicious insiders

Employees or partners who use their legitimate access to corporate data for personal gain

Inside agents

Malicious insiders recruited by external parties to steal, alter, tamper with, or delete valuable data

Disgruntled employees

Emotional attackers who seek to harm their organization as revenge for some sort of perceived wrong

Careless workers

Employees or partners who neglect or ignore the rules of an organization's cybersecurity policy

Third parties

Third-party vendors who misuse their access and compromise the security of sensitive data

hfma ma-ri chapter

New England Healthcare Internal Auditors Inc.

Human Error

Approx. 95% of security incidents are caused by human error:

- System misconfiguration
- Poor patch management
- Use of default usernames and passwords or easy-to-guess passwords
- Lost devices
- Sending sensitive information to an incorrect email address or from a personal email address

hfma ma-ri chapter

New England Healthcare Internal Auditors Inc.

Human Error (more examples)

Double-clicking on an unsafe URL or attachment

Sharing passwords with others

Leaving computers unattended when outside the workplace

Using personally owned mobile devices that connect to the organization's network

hfma
ma-ri chapter

New England Healthcare Internal Auditors Inc.

Password Management Example

Regulatory Response

The New York Department of Financial Services (NYDFS) made a name for itself in the cybersecurity regulatory space in 2017 when it issued 23 NYCRR Part 500, which established cybersecurity requirements for financial services companies that fall under New York State regulation.

On April 14, 2021, the Department of Labor announced new cybersecurity guidelines for plan sponsors, plan fiduciaries, record-keepers, and plan participants to help protect $9.7T in assets.

On May 12, 2021, United States President Joe Biden signed the "Executive Order on Improving the Nation's Cybersecurity (14028)

Regulatory Response

On May 27, 2021, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) issued a security directive on enhancing pipeline security.

On March 9, 2022, the Securities and Exchange Commission ("SEC") proposed rules that would require public companies to make prescribed cybersecurity disclosures. The proposed rules would "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting"

In addition to the executive action being taken, ***the Department of Defense (DoD) has also been making noise in cybersecurity regulatory s***pace with the introduction of the Cybersecurity Maturity Model Certification (CMMC).

hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

FTC Safeguards Rule

Compliance by December 9, 2022

The requirements include, but are not limited to:

- Designate a “Qualified Individual” to oversee the program
- Written Risk Assessment, including a network Vulnerability Assessment (“VA”)
- Written Information Security Program (“WISP”)
- Data encryption (in transit and at rest)
- Multi-Factor Authentication (“MFA”)
- Continuous network monitoring, OR
- Annual penetration testing and twice-annual VAs
- Oversight of Service Providers
- Access Controls
- Annual written report to senior management/ownership

Supply Chain Attacks

Infiltrate One – Impact Many

Breaches Continue to Rise

Supplier Risk is as Real as Internal Risk

Equifax, Log4j, SolarWinds, NotPetya

SOC for Supply Chain

hfma
ma-ri chapter

New England Healthcare Internal Auditors Inc.

Growing Importance of Understanding Outsourcing

Approximately 300,000+ positions are outsourced each year, translating into a $85 billion plus industry worldwide.

Government and Defense sectors are the two largest users of outsourcing in the U.S.

Key areas of outsourcing include IT (54%), finance (44%), payroll (32%) and customer service or contact centers (22%).

65% of businesses using outsourcing say they will consider increasing doing so in the future.

59% of outsourcing firms primarily do so to reduce their overall expenditures.

hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Third Party Risks

Loss of control and communications

Security and privacy concerns

Use of 4th and Nth parties

Responsibilities regarding cyber incidents

Regulatory cybersecurity guidance is increasing
Unanticipated disruptions

hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Third Party Service Provider Selection Tips

Financial, Operational and Reputational Risks

- Obtain financials
- Do a Google search
- Data destruction policy

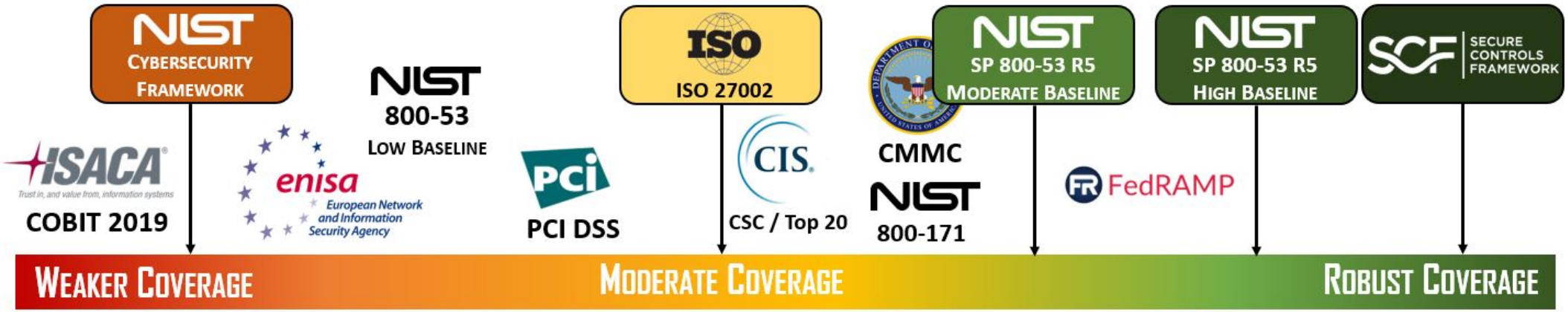
IT Risks:

- Security Questionnaires:
- Inquire if they have a SOC2

hfma ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Security Controls Frameworks



hfma
ma-ri chapter

New England Healthcare Internal Auditors Inc.

Steps to Protect Your (Client's) Organization

How Your Organization/Clients Can Stay Secure

Perform an IT Security Risk Assessment

Provide cybersecurity training

Establish a rigorous vendor management program

vCISO Service Benefits

- Third-Party Provider = Fair Analysis
- Cost-Effective
- Flexibility and Customization
- Breadth of Expertise

Cyber Posture Checklist

Policy & Governance Processes	Effective Processes in Place and Current	Processes in Place but Need Updates or Improvement	Processes Need Major Improvements or Not in Place	Unsure
An individual responsible for the organization's data security meets with leadership (and the Audit Committee) to discuss threats, security control metrics, and ongoing risk mitigation efforts				
Critical security related practices and policies (password changes, privileged account access, etc.) are documented and reviewed annually				
Cyber risk training and awareness for all employees is ongoing				
A tested and reliable disaster recovery/business continuity plan where data and systems can be recovered and made operational				
An incident response plan that is periodically tested and can be executed once a security event/incident has been detected				
Periodic independent assessments against a holistic Security Controls Framework (e.g., NIST, CIS 20, etc.) are conducted routinely				

Cyber Posture Checklist

Tactical Areas of Focus Processes	Effective Processes in Place and Current	Processes in Place but Need Updates or Improvement	Processes Need Major Improvements or Not in Place	Unsure
A vendor management program that routinely reviews security practices for service providers that process or store critical and sensitive information				
Social engineering and phishing simulations are performed periodically to assess training and awareness				
Threats, including Ransomware, are assessed periodically with proper risk mitigation				
Security patches for all network devices, software, and applications are routinely cataloged, prioritized, and scheduled for timely update				
Internal vulnerability scans are performed routinely to identify internal system weaknesses				
Remote access to the network requires Multi-Factor Authentication (MFA)				
Outside network penetration is periodically attempted via an outside vendor in an effort to find weaknesses				
Management has policies relative to the use BYOD (Bring Your Own Device) such as cell phones				
Cyber insurance is currently in place				

QUESTIONS

hfma
ma-ri chapter