ANCHIN

Accountants and Advisors

Financial Services Coffee Chat

Cyber Considerations for the Financial Services Industry
Presented by: Russell Safirstein
President & CEO: Redpoint Cybersecurity, LLC
June 15, 2021

RUSSELL S. SAFIRSTEIN

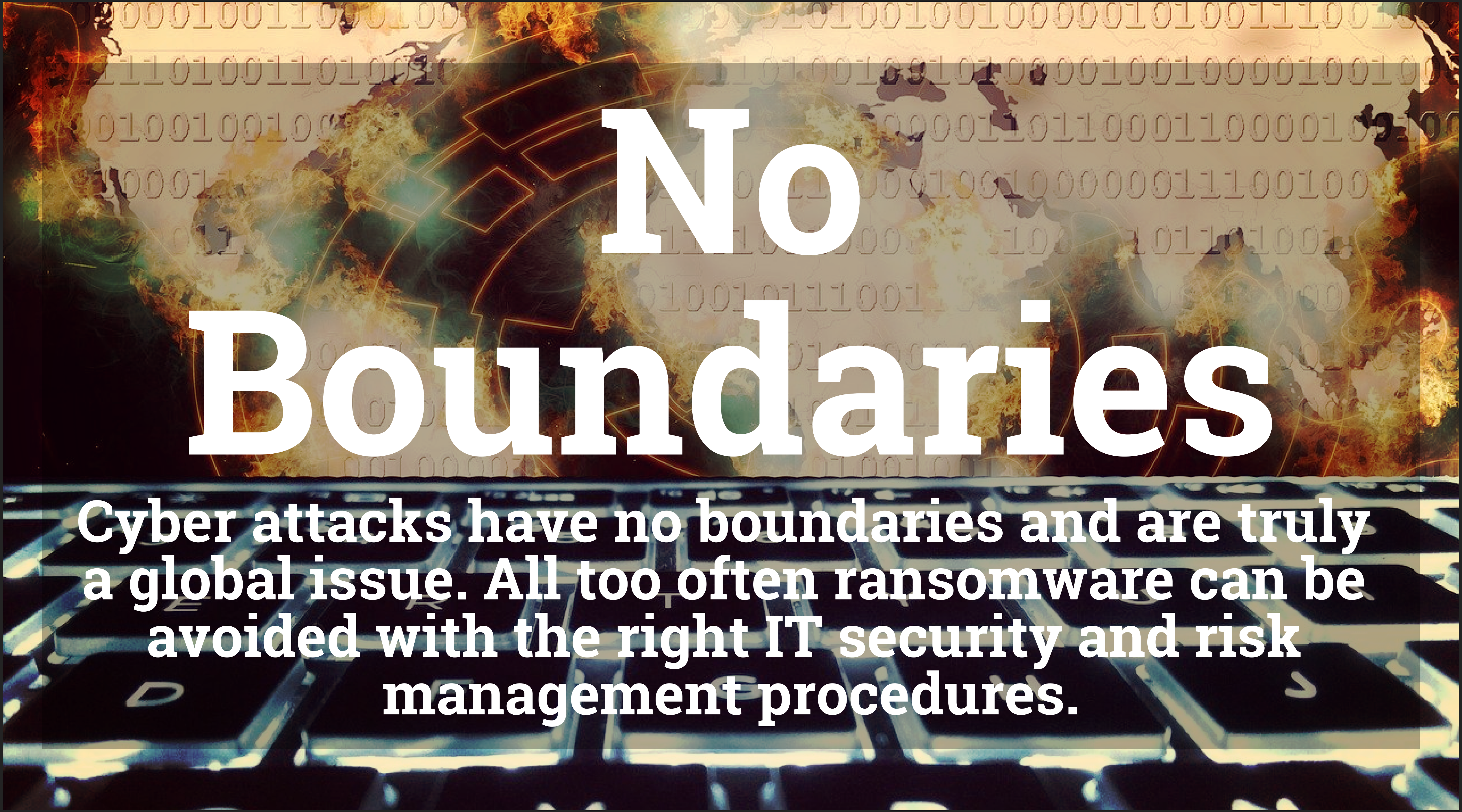
Russell Safirstein is President and CEO of Redpoint Cybersecurity, LLC Redpoint is a subsidiary of Anchin where he is also the Partner in Charge of Anchin Digital Risk Solutions. He is a senior executive and a progressive thinker with over 30 years of experience and has been successful in bringing non-traditional solutions to an ever-changing work environment. Russell has co-founded several organizations that specialize in AI & Machine Learning and holds several patents. Russell is a highly regarded and sought after speaker on cyber security, technology, audit and risk practices.

Prior to his current roles, Russell was a Partner for a mid-size accounting firm leading their AI and Machine Learning initiatives, in addition to their cybersecurity and risk advisory practices and President of a technology risk consultancy firm where he led the development of its AI platform. He held several Chief Audit Executive roles for several global organizations Mr. Safirstein started his career with KPMG in their Financial Institution practice after graduating from Adelphi University with a BBA in Accounting.

Would you know if a hacker was in your network, or email, or phone, right now?

NAVIGATING CYBERSECURITY IS DIFFICULT

Protect what matters most



No Boundaries

Cyber attacks have no boundaries and are truly a global issue. All too often ransomware can be avoided with the right IT security and risk management procedures.

What's Next?

Solar Winds

First became aware of the SolarWinds breach through a December 2020 breach to FireEye, a major cybersecurity firm, by nation-state hackers.

This was part of a much larger attack that is believed to have started in March 2020 which was carried out through malicious updates to a popular network monitoring product and impacted major government organizations and companies.

Microsoft Exchange

At least 30,000 organizations were compromised beginning on January 6, 2021 by Chinese unit by exploiting flaws in Microsoft Exchange Server email software.

Fixed via an emergency security update on March 2nd.

Any organization who was running self-hosted Outlook Web Access was hit with a zero-day attack.

Colonial Pipeline

The hacking of Colonial Pipeline, likely by DarkSide, a Russian cybercrime gang.

Clear indicators of the poor state of cybersecurity in much of the critical infrastructure in the U.S.

Ransomware = Terrorism

New U.S. DOJ initiative elevates ransomware to similar priority as terrorism

Centrally coordinated

New task force to connect the dots

Expanded ecosystem

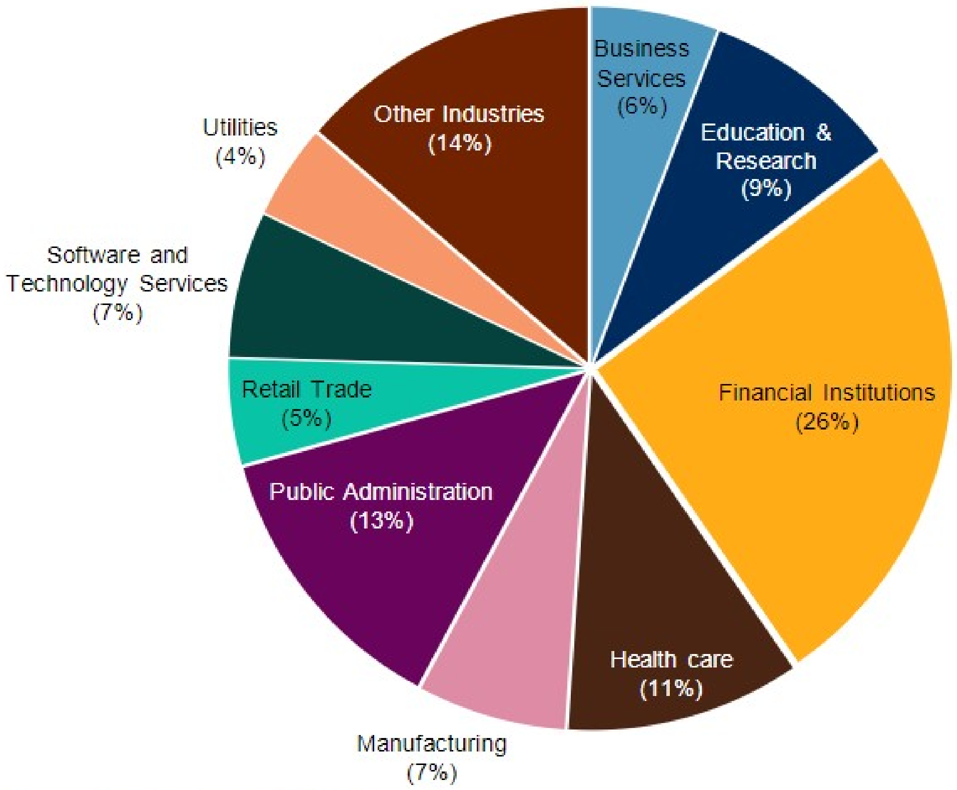
Includes counter antivirus, illicit online forums, cryptocurrency, bulletproof hosting services, botnets and online money laundering services.

Private Sector needs to step up

“No company is safe from being targeted by ransomware, regardless of size or location.”

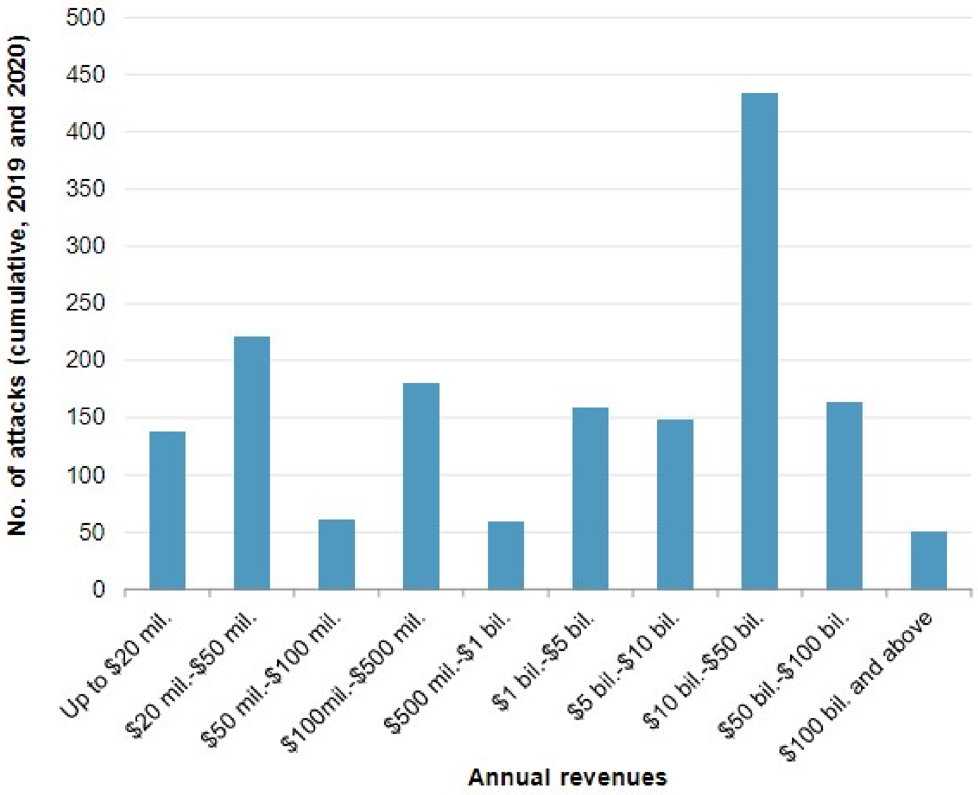
Financial Industry The Most Frequent Cyber Attack Targets In The Past Five Years

Industries share in cyber events, cumulatively 2016-2020



Source: Guidewire, S&P Global Ratings.

Financial Institutions With $10 Bil.-$50 Bil. Revenue Had The Highest Number of Attacks Over The Past Two Years



Source: Guidewire, S&P Global Ratings.

NYDFS Cybersecurity Regulation

23 NYCRR 500

- **Any institution that needs a license from the NYDFS is covered by this regulation**
- **Exemptions**
  - Fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or
  - Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or
  - Less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, or
  - There's no storing or processing of nonpublic information.

- **What is being asked?**
  - NYDFS is asking organization to assess their security risks, and then develop policies for data governance, classification, access controls, system monitoring, and incident response and recovery.
  - Need to designate a CISO who will annually sign off on the organization's compliance.

Data Privacy

Emerging Trends

- **No Federal Law**
  - More and more states are requiring data protection and privacy plans.
  - All 50 states have breach notification statutes.
- **PII = Moving target**
  - Definition expansion with each passing new regulation. Different standards per state and EU
- **Know your data and where it lives within the organization**
  - You need to reassess based on WFH
- **Document everything**
  - Plans, policies, procedures, programs, etc.

- **NYS Shield Act**
  - Effective as of March 21, 2020, New York enacted one of the most aggressive state data breach notification laws in the United States, the “Stop Hacks and Improve Electronic Data Security” (SHIELD) Act.
  - This law applies to any person or business (even those operating outside of New York) that collects and maintains New York residents’ “private information.”
  - **Exemptions**: fewer than fifty employees; less than three million dollars in gross annual revenue in each of the last three fiscal years; or less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles (GAAP).
  - An applicable businesses must still maintain a security program, and adopt ”reasonable” administrative, technical and physical safeguards based upon the size and complexity of its operations, scope of activities and the sensitivity of the personal information the small business collects.

Enforcement Actions

- ## HIPAA

  Post Data Breach: Following a data breach and subsequent investigation, a Georgia orthopedic clinic paid $1.5m to the Office of Civil Rights to adopt a corrective action plan to settle potential violations of HIPAA Privacy & Security Rules.

- ## NYS DFS 500 Regulation

  Failure to Properly Remedy: First American Title, one of the largest title insurance providers in the country, were charged with exposing hundreds of millions of documents after they persisted for years (since 2018).

Types of Data Breaches

- ## Denial of Service

  Denial-of-Service attacks occur when a website is **overwhelmed** with requests, which blocks other users from the site.

- ## Business Scams/Phishing

  Acquire data from disparate resources, like commercial email clients **(Gmail, Microsoft Outlook)** to investigate for **Business Email Compromise (BEC)** and determine affected data and origin.

- ## Insider Threat/Employee Misconduct

  Conduct investigations for cloud based social media accounts **(Facebook, Instagram, Twitter, LinkedIn)** affording clients visibility into potential employee misconduct affecting company reputation.

- ## Data Theft

  Leverage forensics to investigate the **exfiltration** of digital evidence to verify if a compromise occurred, create a timeline of events, and determine attribution in the incident.

- ## Malware

  Any type of virus, including worms and Trojans, is malware.

- ## Ransomware

  A hacker gains control of the company system and locks it from use. A ransom note is left within the virus. The company or user is extorted to pay money for data to be restored or their data is destroyed.

What are the Biggest Threats?

Much broader than just "cyber"

- **Employee error**

  Employees are the weakest link in your data breach defense. Your organization is just one click away from having its data and systems hijacked.

- **Cyber attack**

  Can use exploits to access to sensitive information and/or use malware to gather sensitive information or cause business disruptions.

- **Social engineering**

  The most common form of social engineering is phishing.

- **Unauthorized access**

  Information from inside your premises.

- **Ransomware**

  It's a type of malware that encrypts files and blackmails the infected organization into handing over money to receive the decryption key.

- **Malicious insider**

  Malicious insiders tend to be motivated by revenge or financial gain.

- **Physical theft**

  Not all data breaches relate to digital information. Organizations also need to be concerned about physical theft – namely paper records and devices that provide access to sensitive information.

Two Factors Account for Most Theft and Loss

Compromises in Insider Accounts

Exacerbated by far wider employee and third-party access to sensitive information than was necessary

Failure to monitor

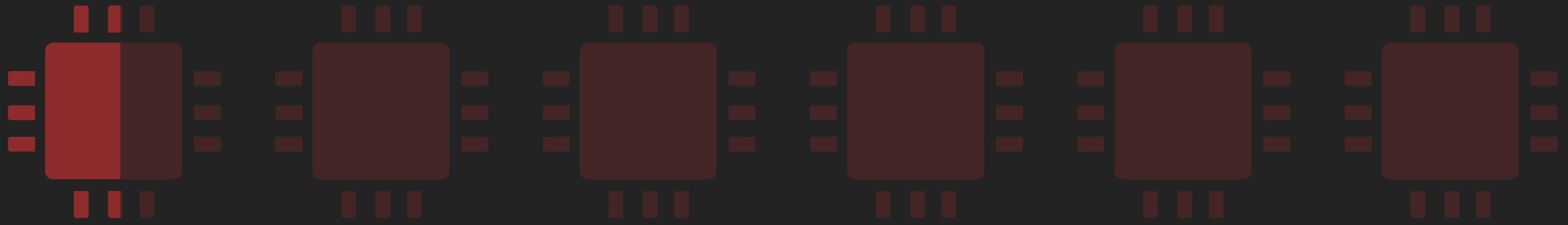
Access and activity around email and file systems was not monitored

What causes most Cyber Breaches?

90%

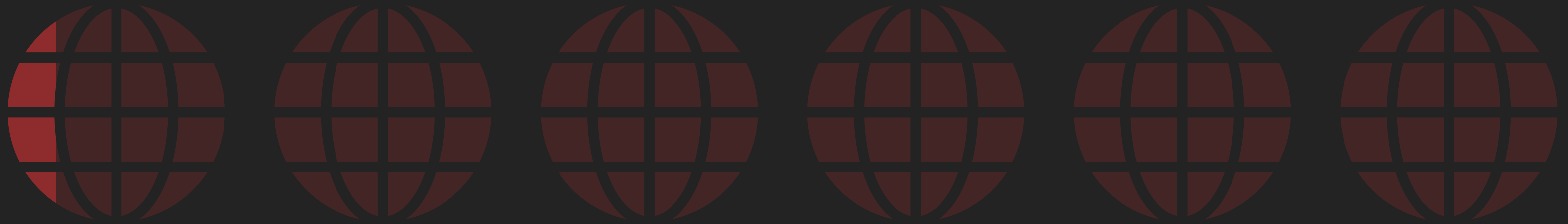
People

7%



Technology

3%



Dark Web or Similar

Redpoint
Cybersecurity LLC

Pandemic's Lasting Impact

Risks abound about the very survivability of organizations

- Unprecedented challenges brought by the COVID-19 pandemic as well as expanding reliance on technology and data collection are driving business continuity/crisis management and cybersecurity as top-rated risks
- Business continuity/crisis management and cybersecurity were the two most relevant risks
- Work-from-home environment introduced the monumental task of enforcing cyber-safety protocols for entire offsite workforces
- Changes to operations, mitigating the vulnerabilities of popular communications software, managing customer and vendor relationships strictly online, and internal audit's inability to perform on-site visits.

...What is impacted? Cybersecurity budgets...

Redpoint Cybersecurity LLC

A Brief Update: Early 2021

Cyber Extortion - Ransomware

- **15% of American business negotiate ransom payments**

  Ensure compliance with regulatory bodies: FINRA, FinCEN, FBI, and other government entities.

- **Ransomware costs $646k per breach**

  Understand how **adversary TTPs** operate to aid in negotiations in determining sophistication and impact.

- **20% of Ransomware victims were SMBs in 2020**

  Elevate and support local enterprise competencies for SMBs.

- **200% Yearly Cost Increase**

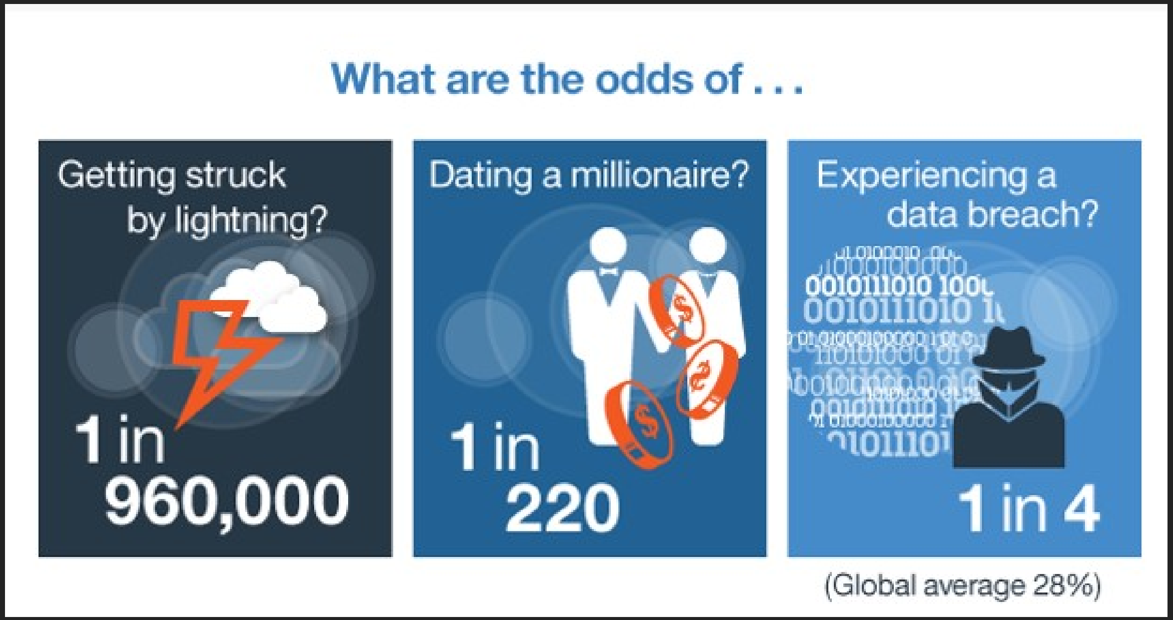
  Need to contain the effects of ransomware and proactively hunt for indicators attackers exploited thereby **lowering and controlling costs to the client.**

Cybersecurity its a journey

...but first we need to debunk a few myths

Myth #1

"We're Not At Risk... We're too small to be a target."



60% of small to mid-size businesses have been targets of cyber crime.

Myth #2

"If the attackers want to get in, they'll get in. There's nothing we can do to stop it."

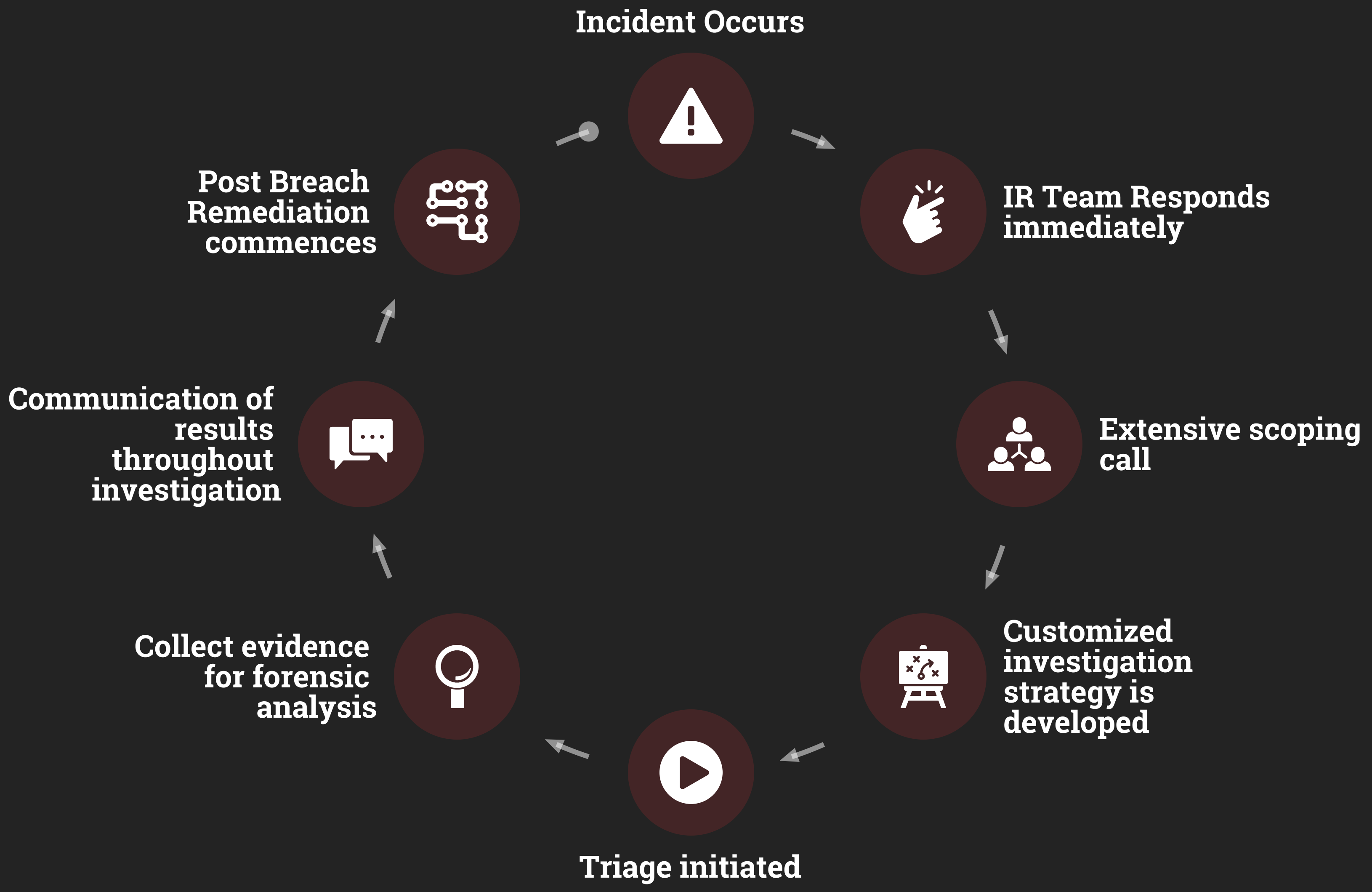
100% security does not exist.
0% risk does not exist

You need to be offensive rather than defensive to protect your organization

Myth #3

“We have IT. It's their problem not mine.”

Cybersecurity is everyone's responsibility not just IT.



Incident Occurs

IR Team Responds immediately

Extensive scoping call

Customized investigation strategy is developed

Triage initiated

Collect evidence for forensic analysis

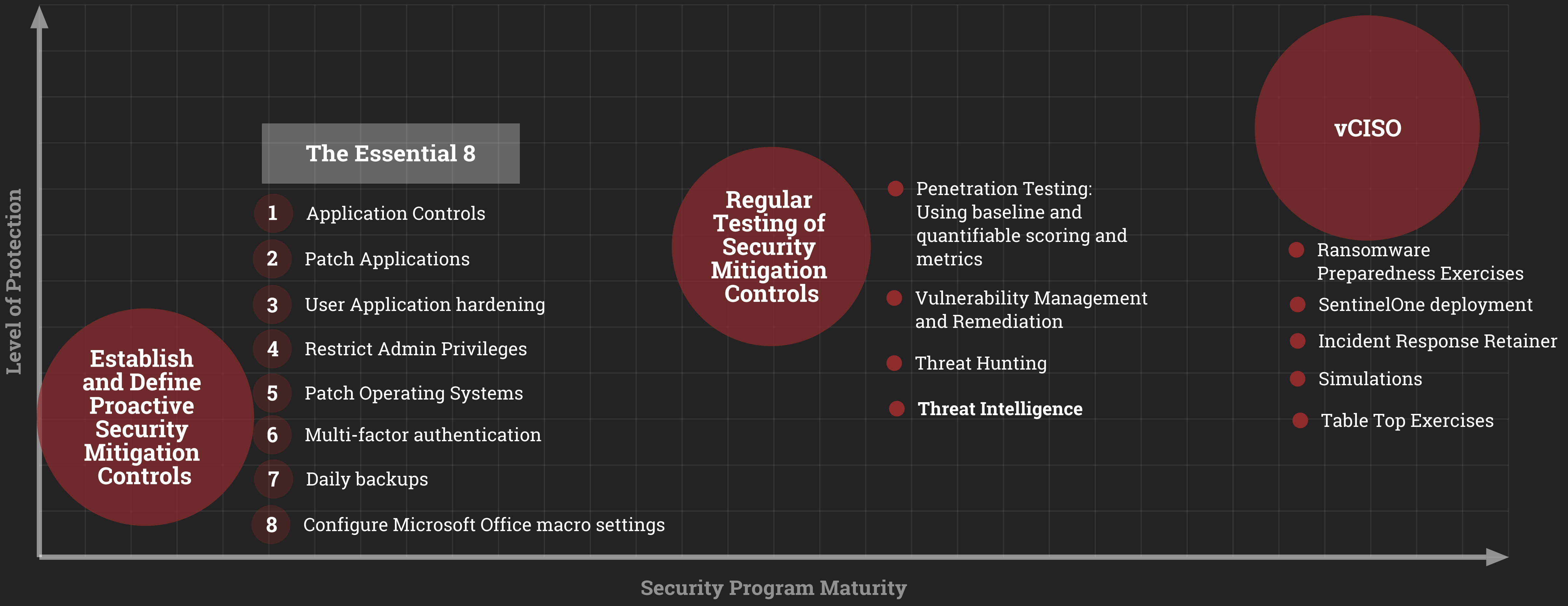
Communication of results throughout investigation

Post Breach Remediation commences

Incident Response Methodology

A Practical Approach to Mitigating Threats

Redpoint Cyber: Security as a Service Offering



Establish and Define Proactive Security Mitigation Controls

The Essential 8

1. Application Controls
2. Patch Applications
3. User Application hardening
4. Restrict Admin Privileges
5. Patch Operating Systems
6. Multi-factor authentication
7. Daily backups
8. Configure Microsoft Office macro settings

Regular Testing of Security Mitigation Controls

- Penetration Testing: Using baseline and quantifiable scoring and metrics
- Vulnerability Management and Remediation
- Threat Hunting
- **Threat Intelligence**

vCISO

- Ransomware Preparedness Exercises
- SentinelOne deployment
- Incident Response Retainer
- Simulations
- Table Top Exercises

Redpoint Cybersecurity LLC

Essential 8

Daily Backups

- Ensure **important information** such as new/changed data, software and configuration settings can be accessed following a cyber security incident (e.g. a ransomware incident).
- More than 20% of small to medium sized.businesses will suffer a major disaster causing loss of critical data every 5 years
- **93% of companies that lost their data for 10 days or more filed for bankruptcy** within one year of the disaster, and 50% filed for bankruptcy immediately

Essential 8

Multi-factor Authentication

- **Stronger user authentication,** including for VPNs, RDP, SSH and other remote access,and for all users when they perform a privileged action or access an important/sensitive data repository, makes it harder for adversaries to access sensitive information and systems.
- 81% of breaches are due to weak or stolen passwords such as common phrases or repeated words/numbers
- **Phishing emails are successful nearly half of the times** they are carried out.
- An average employee has to remember approximately 27 passwords.

Essential 8

Restrict Admin Privileges

- Admin accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems. Privileges to operating systems and applications should be restricted based on user duties and regularly revalidated based on the need for privileges.
- **In 2019, 34% of data breaches involved internal actors.**
- Of all the attacks organizations experience, **99.9% of those exploiting a known vulnerability** occur more than a year after the publishing of the associated CVE (Common Vulnerabilities and Exposures).

Essential 8

Patch Operating Systems

- Vulnerabilities in operating systems can be used to further the compromise of systems.Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours, use the latest OS, and do not use unsupported versions.
- 20% of all vulnerabilities caused by unpatched software are classified as High Risk or Critical.
- 80% of companies who had a data breach or failed audit could have prevented it with patching or configuration updates.
- **57% of data breaches are attributed to poor patch management**

Essential 8

Application Control

- To prevent the execution of malicious programs (including .exe, DLL, scripts) and installers, **all unapproved applications are prevented from executing.**
- Whitelisting application allows protection against ransomware and other types of malware attacks. Traditional anti virus software tends to be signature-based.Whitelisting also helps decrease help desk costs, giving IT staff the ability to make sure that users are running application versions that are known to be stable and reliable.
- The top malicious email attachment types are .doc and .dot which make up 37%. The next highest is .exe at 19.5%.

Essential 8

Patch Applications

- Security vulnerabilities in applications (e.g. Flash, web browsers, Microsoft Office, Java) can be used to execute malicious code on systems.
- 92% of web applications with security flaws or weaknesses that can be exploited
- 18% of all network-level vulnerabilities are caused by unpatched applications

Essential 8

User Application Hardening

- Flash, ads and Java are popular ways to deliver and execute malicious code on systems. Web browsers can be configured to block or uninstall all three, and unnecessary features (e.g. OLE and PDF viewers) can be disabled.
- 61% of organizations have experienced an IoT security incident, with IoT devices experiencing an average of 5,200 attacks per month.
- **Nearly 90% of usage on mobile phones and tablets occurs through apps. The prevalence of the Internet of Things and increasing use of personal devices invulnerable sectors have made the need for application hardening urgent.**

Essential 8

Configure Microsoft Office Macro Settings

- Macros can be used to deliver and execute malicious code on systems. The right settings can block macros from the internet and only allow vetted macros in 'trusted locations' with limited access or trusted certificates.
- In the enterprise, recent data from our Office 365 Advanced Threat Protection service indicates **98% of Office-targeted threats use macros.**
- Despite periodic lulls, infections for the top 20 most detected macro based malware were high over the past three months.

Redpoint Cyber: Who We Are

- **30+ Elite Cyber Security Experts with Nation State Experience**

  Active Security Clearances

  18 years average U.S. Government Experience

- **92% Have Advanced Degrees**

- **Incident Response Experts with Breach and Legal Investigation Expertise**

  450+ Successful Operations

- **Advanced Certifications**

  GIAC Certified Intrusion Analyst

  Certified Ethical Hacker

  Certified Fraud Examiner

  CISSP

  DCITA Certified Incident Responder

  GIAC Certified Forensic Examiner

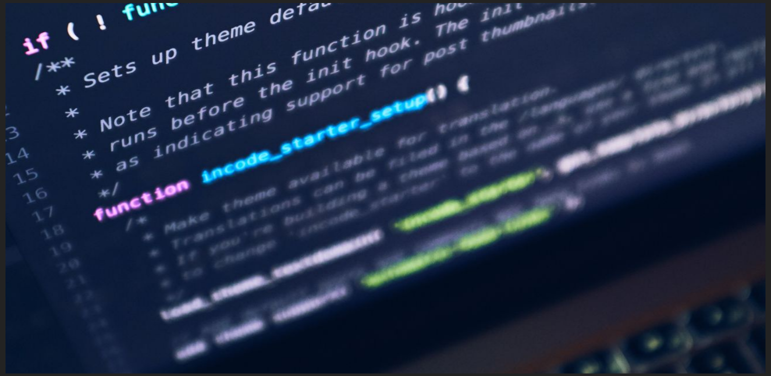
  GIAC Certified Incident Handler

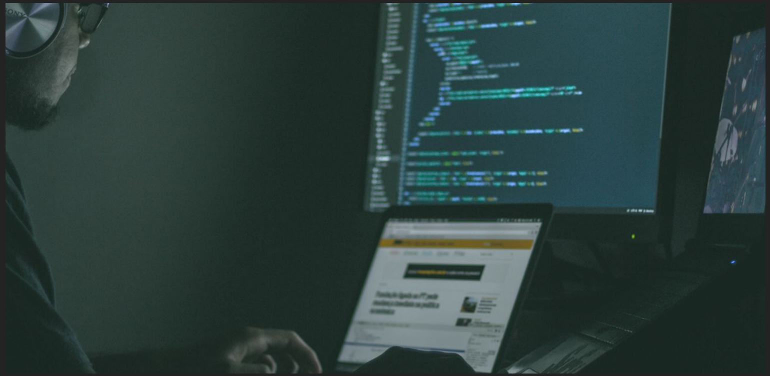
  GIAC Reverse Malware Engineer

  AWS Cloud Certified Practitioners

  AWS Solutions Architect

What Redpoint Does





Breach Response Services

Digital Forensics & Incident Response

IR Triage & Investigation Support

Program Transformation and Operations Optimization

Post Breach Recovery and Remediation

Threat Mitigation Services

Threat Hunting

Penetration Testing / Ethical Hacking

Threat Intelligence

Ransomware Preparedness Exercise

Attack Surface Visibility Analysis

Cloud Security Consulting

Secure Cloud Migration

Cloud Security Assessment & Roadmap

Compliance

Data Protection

Infrastructure Protection

Why We Are Different

Human Led

Nation State Experience

Advanced Training

Certified and Tested Experts

Classified Mission Specialists

Technology Enabled

Optimize Client Existing Technology Investments

Investing in Emerging Capabilities and Tools

Tradecraft

Automated Malware Detection and Remediation

Consistent and Repeatable Process - Hunt & IR methodology based on NSA CIRA

Agility

Hybrid (remote and onsite) approach to Hunt & IR

Simple and Easy to Start Hunt & IR engagements

ANCHIN
Accountants and Advisors

Redpoint
Cybersecurity LLC

Russell Safirstein

russell.safirstein@anchin.com

russell@redpointcyber.com

212.863.1231