HPA | HighPoint Associates

Cybersecurity Diagnostic Overview

February 2019

WHY FOCUS ON CYBERSECURITY? (1 OF 3)

Data Breach Examples*:

EQUIFAX

YAHOO!

ASHLEY MADISON®.COM

Healthcare Services Organization with Stolen Laptop Containing 2.8M Personal Health Records: $1.6B cost**

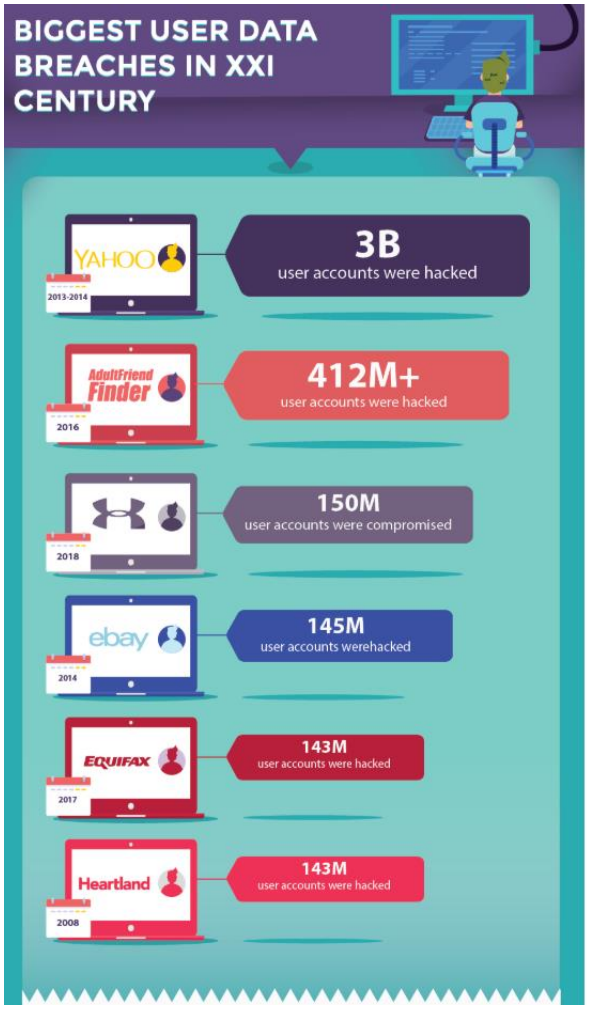
Tangible Costs	+	'Hidden' / Intangible Costs
• Customer breach notifications ($10M) • Post-breach customer protection ($20M) • Regulatory compliance and fines ($2M) • PR / crises communications ($1M) • Attorney fees and litigation ($10M) • Cybersecurity 'rush' improvements ($10-20M) • Technical investigations ($1M)		• Operational disruption ($30M) • Lost value of customer relationships (~$430M) • Lost contract or recurring revenue (~$830M) • Loss of IP (N/A) • Devaluation of trade name ($230M) • Higher cost to raise debt ($60M) • Insurance premium increases ($40M)

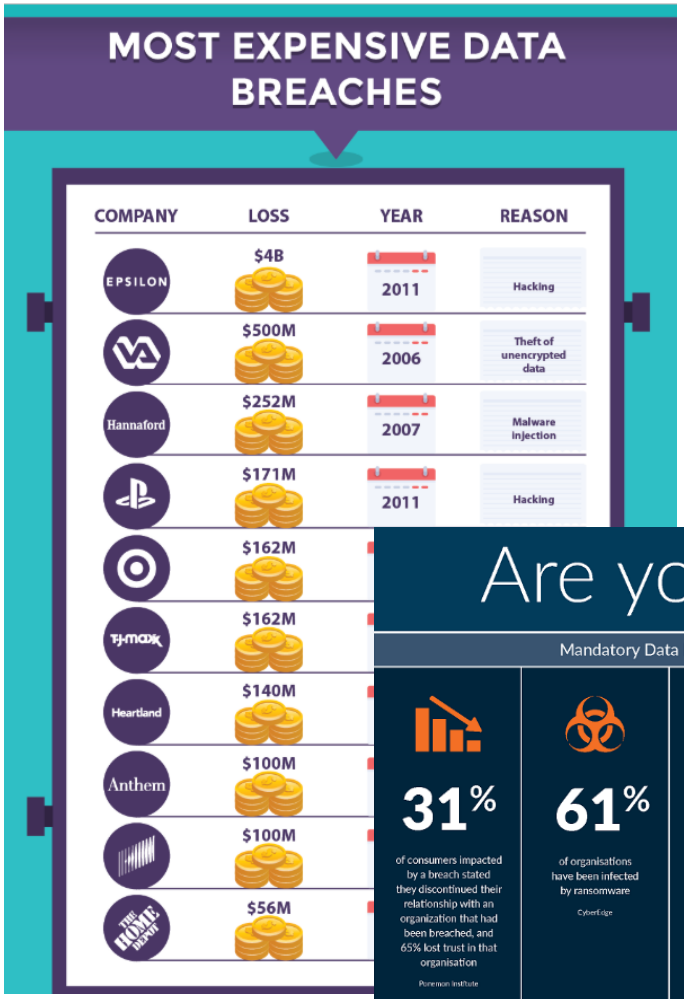
HPA

*Note: Data breaches are only one type of negative cybersecurity outcome; many others such as hijacking of IoT or Denial of Service (including ransomware) are connected to business failures and costs
Sources: *CSO Magazine* / **Deloitte representative sizing

WHY FOCUS ON CYBERSECURITY? (2 OF 3)

Recent Infographics paint the headlines…





Sources: EveryCloud 2018 Cybersecurity Infographics

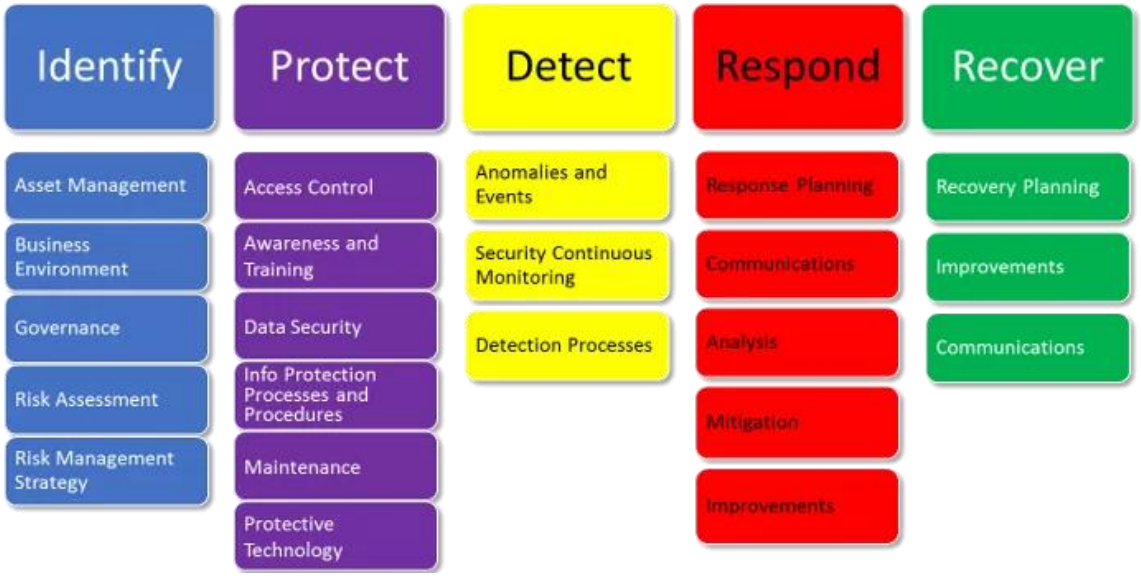
WHY FOCUS ON CYBERSECURITY? (3 OF 3)

- Cybersecurity is consistently ranked as the **#1 risk facing any organization**
- Cybersecurity is **no longer just an IT issue**, and **ownership must be taken across the organization**. Prior to ownership, there needs to be **understanding**
- There is **no silver bullet technology**, nor is a silver bullet likely as long as there are users. In fact, **risks will continue to grow** as Information Technology and the Internet of Things become increasingly pervasive across all industries
- Cybersecurity **incidents will and do happen** even to the most prepared and resourced organization. **Goal is to reduce the number, frequency and impact**
- The **average time to detect a data breach is 206 days and rising**, with 53% of breaches being detected outside of the organization. These trends need to be reversed to reduce the risk that breaches become terminal events
- Responding to an incident needs **advance planning and practice**. **Lack of preparation increases costs** both direct and indirect and slows recovery. Organizations need to be **prepared from the top down**

HPA

THE NIST CYBERSECURITY FRAMEWORK (NIST CSF) (1 OF 2)

In response to the increasing threats presented to US and global economies by cybersecurity, the National Institute for Science and Technology was given the charter to create a single universal framework for use by commercial, federal, state and local organizations. This framework, known as **NIST CSF**,* has become the leading model for how IT thinks about Cybersecurity. It consists of standards, best practices, and recommendations split into 5 subject areas. Within each subject area, there are 3-6 sub areas…



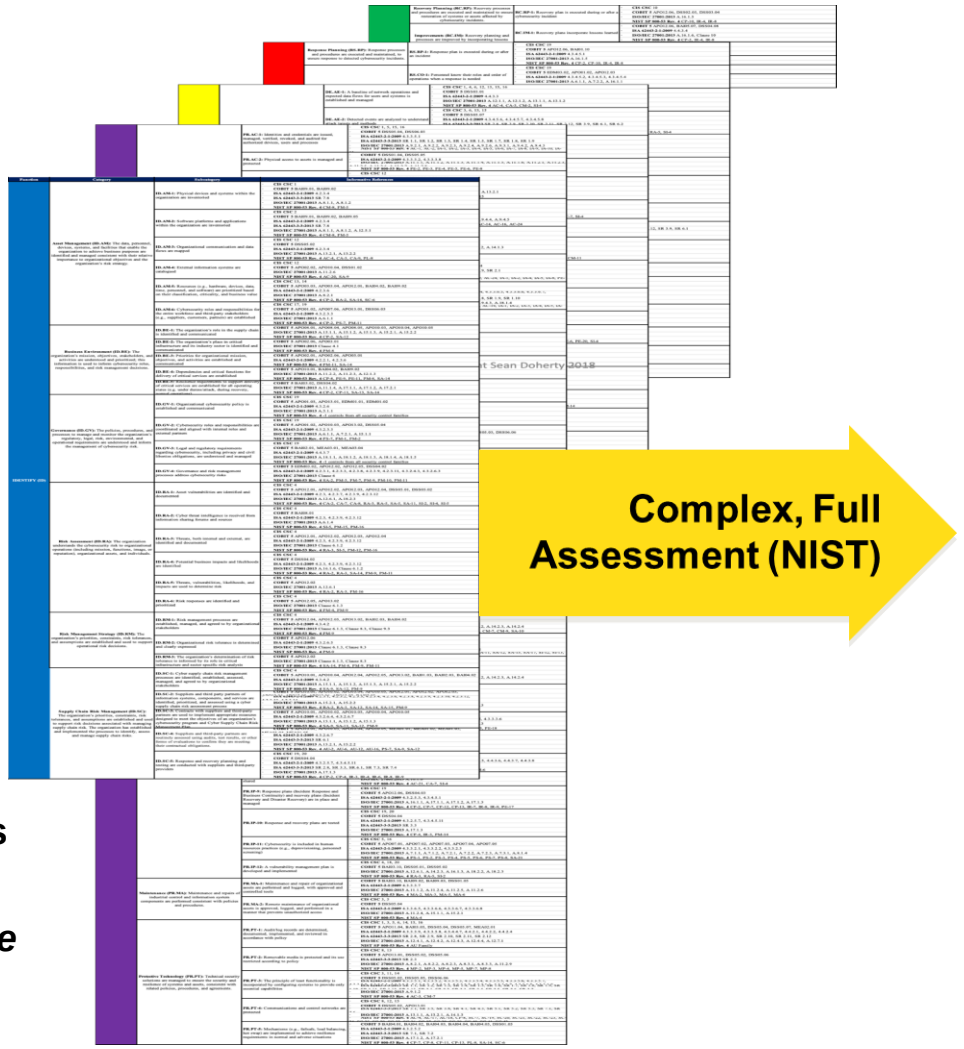
*NIST CSF is designed to compliment existing frameworks including; ISO 27001/2 with focuses on the security management system, PCI DSS for systems around payment card data , CIS Critical Security Controls which details 20 mainly defensive technical controls and HITECH with specific provisions for Healthcare, but has the breadth and depth that means over time it will likely replace them in whole or in part.

HPA

THE NIST CYBERSECURITY FRAMEWORK (NIST CSF) (2 OF 2)

The high-level **design of the NIST CSF is very simple and logical, but hides complexity.**

The summary of NIST CSF 1.1 runs to 48 pages, details **108 sub categories each of which contains 6-23 controls**. Each control details specific actions that align with a standard, best practice or recommendation.



<u>Effective but complex and timely framework</u>*: Most organizations struggle to know where to start when adopting NIST CSF, and fail at the first hurdle of assessing themselves against its breadth and depth

Full assessments are 1 year+ and tens of people

*Note: NIST offers a framework rather than a prescriptive recipe. It is limited to a framework as there is continuous, dynamic change in cybersecurity

THE HPA SIMPLIFIED CYBERSECURITY SOLUTION

	Simplified, Leading Indicators (HPA Approach)	**Complex, Full Assessment (NIST)**
Resource Intensity:	• Focused team of 2-4 FTEs • ~2-3 months diagnostic / rectification plan	• 10-100 FTEs • 1+ year full diagnostic review
Primary Approach:	• 10 focused leading indicator assessments - Each leading indicator has a representative query behind the simplistic indicator • Ultimately reads out on Maturity, Fitness, and Incident Readiness • Feeds into NIST assessments	• Thousands of controls / assessments • Potential to mis-prioritize higher and lower priority issues observed

Simplified approach, NOT fully representative of NIST; Approach is a rapid cybersecurity health check based on assessment of HPA Subject Matter Experts and experience with like firms

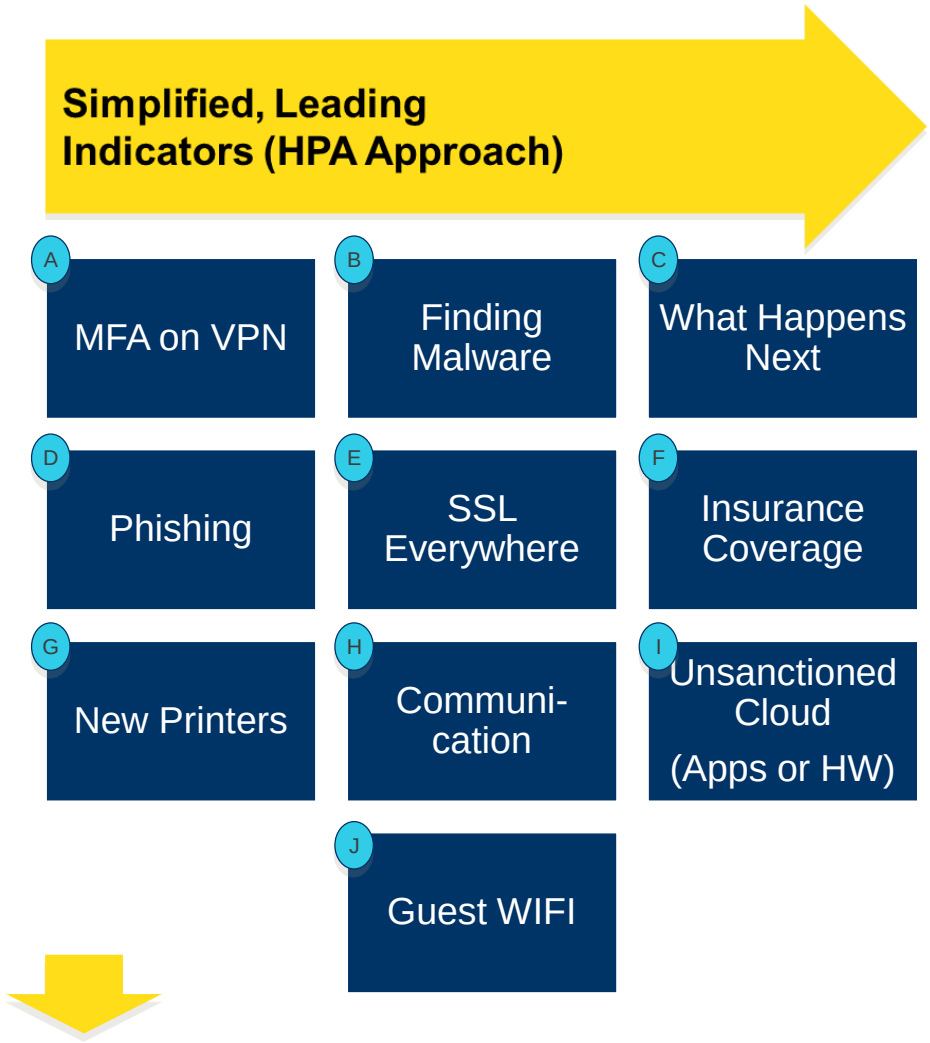
HPA

HPA CYBERSECURITY LEADING INDICATOR APPROACH

HPA believes in the value of adopting the NIST CSF, yet **understands the need to get started by quickly assessing an organization's cybersecurity posture**. A leadership team's ability to identify and prioritize actions to increase the cybersecurity posture is severely compromised without this early analysis.

HPA, partnering with leaders in Cybersecurity, has identified **TEN Leading Indicators of cybersecurity posture** that **feed into a model supporting NIST CSF adoption**.

Each indicator provides **insights into the short and medium term actions that can be taken** to improve cybersecurity.



Simplified approach is not fully representative of NIST as it omits more advanced topics like micro-partitioning or code security – this is a first health check

HPA CYBERSECURITY LEADING INDICATORS HAVE REPRESENTATIVE QUERIES

Simplified, Leading Indicators (HPA Approach)

- Each leading indicator focuses on **easy-to-understand topics**, removing the abstract
- **Employees at all levels can quickly engage** with the topics and **understand both the diagnostic and also the larger question / derived actions**
- Diagnosing these 10 topics provides an **efficient mechanism to create an understanding of a much wider set of controls and processes**
- There are **areas of NIST CSF and other frameworks not covered by design:**
  - e.g., the results of vulnerability scans or secure code reviews are valuable tools, and encouraged, but they do not inform the Maturity, Fitness and Incident Readiness of the organization
  - Organizations that use external vulnerability scans and penetration tests as a proxy often evaluate poorly across the diagnostic

	Representative Queries Behind
A MFA on VPN	• How widely deployed is Multi-Factor-Authentication / how protected is **access to a variety of infrastructures and systems** including cloud computing?
B Finding Malware	• How does the firm detect malware? **What kinds are being detected, and how automated is the response?** How are **exceptions incorporated** in the go-forward?
C What Happens Next	• How **familiar is the organization at recognizing Cybersecurity incidents**, and how prepared is the organization to react to them?
D Phishing	• To counter email and social media attacks, **what portion of the organization reflects training?** How does the organization **report attacks**?
E SSL Everywhere	• How **secure are our communications** across networks, both within the organization, and with sanctioned cloud services?
F Insurance Coverage	• In the event of a breach, **do we have appropriate coverage to mitigate costs**, with contingency funds and **access to specialist resources**?
G New Printers	• How does the organization **manage infrastructure, endpoint management and privileged account access** using printers as a proxy?
H Communi-cation	• What are the **roles and policies that have or are yet to be defined**, as well as the **quality and usefulness of what is currently communicated**?
I Unsanction-ed Cloud	• What are the **incidences and controls on unsanctioned technologies**? How do they reflect more broadly **cloud and other addition procedures**?
J Guest WIFI	• How is **network access granted? Guest WIFI managed?** Both are proxies for basic intranet and internet security …

HPA

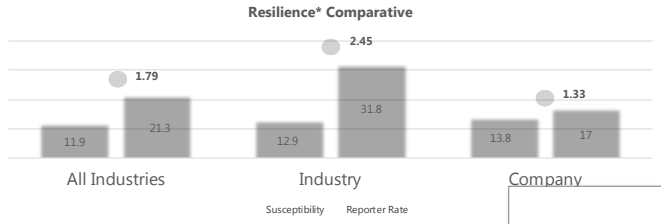
SAMPLE LEADING INDICATOR OUTPUT

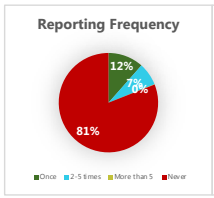
D

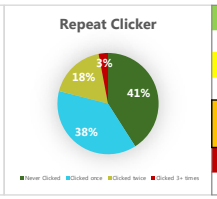
Phishing

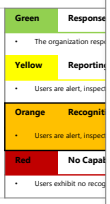
Simplified, Leading Indicators (HPA Approach)

PHISHING SUMMARY









The Resilience score of 1.33 is below both the industry and all industry benchma
awareness of email threats but are poor at reporting them. Those who are unaw
high risk behaviors with 21% of the user population clicking 2 or more phishing

*Resilience - Number of reported / Number of susceptible. Lower susceptibility + higher reporting = better resiliency.

HPA

PHISHING RECOMMENDATIONS

Observations	Recommen
59% of user population was shown to be susceptible to one or more Phishing simulations	Develop tools be simulati
19% of users reported a phishing simulation using the correct channel. In interviews users reported not understanding who to and how to report suspicious emails. Confusion over the use of the "Security" email alias was common.	Re-laun Incorpo Drive re as the c
Interviews consistently showed that users were only familiar with general phishing types. None of the users interviewed had knowledge of specific attacks facing Industry	User aw
Management who had awareness of BEC gained knowledge from external media only and had not been shown example common in Industry	SME pr entry or
This was the first time a Phishing Simulation had been conducted. Data collected has already been used to inform SecOps.	Evaluate

*Resilience - Number of reported / Number of susceptible. Lower susceptibility + higher reporting = better resiliency.

HPA

CONFIDENTIAL 3

For this illustration: Over a 2 week period, 10 Phishing scenarios were deployed in a phishing simulation - 4 scenarios were generic and 6 specific to the client's industry. The results showed that the client had issues in susceptibility (likelihood to be duped) amongst both a subset of employees and reporting rates generally. Interviews with employees and management also showed a lack of knowledge on the types of attack common in the industry and confusion over how to take action

HPA

SAMPLE LEADING INDICATOR EFFICACY

G

New Printers

Simplified, Leading Indicators (HPA Approach)

Principle of Least Privilege (PoPL)

Printers are often a common reason for delay/failure when implementing the PoPL for operating system administrator rights. We use the lens of Printer management to asses how well the firm has implemented PoPL for desktop OS administration as well as other controls associated with print infrastructures such as software and hardware supply chain.

⟶ **This strategy has been shown to protect against 95% of critical Windows vulnerabilities***

'How do you install a new printer?' Drives Understanding of:

- The firm's implementation of PoPL for desktop operating system admin. rights (completeness, exceptions, roadmap to complete)
- Controls on vendor supplied software: with printer drivers and management software as the example
- Controls on hardware supply chain: with local printers and print service providers as the example
- Controls for Multi-Function Devices within the firm: hardening, configuration, logging, physical security, hard disk controls
- Preparedness for managing an incident involving the print infrastructure: with malware in a printer driver as the example

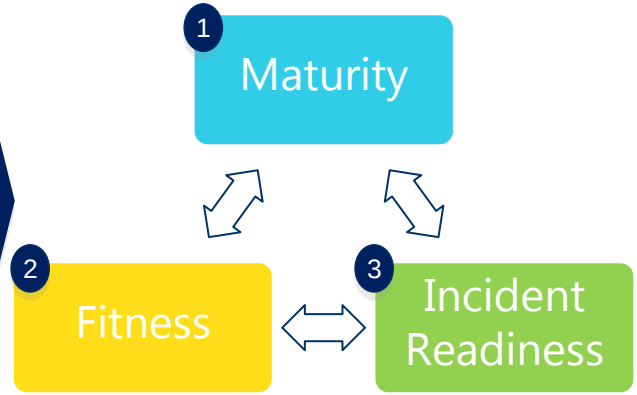
HPA

*Sources: Gartner/Avecto 2018 in Beyond Trust 2018 https://www.beyondtrust.com/blog/entry/research-reveals-microsoft-vulnerabilities-more-than-doubled-since-2013

LEADING INDICATORS LEAD TO 3 EVALUATIONS

Simplified, Leading Indicators (HPA Approach)

		Representative Queries Behind
A	MFA on VPN	• How widely deployed is Multi-Factor-Authentication / how protected is **access to a variety of infrastructures and systems** including cloud computing?
B	Finding Malware	• How does the firm detect malware? **What kinds are being detected, and how automated is the response?** How are **exceptions incorporated** in the go-forward?
C	What Happens Next	• How **familiar is the organization at recognizing Cybersecurity incidents**, and how prepared is the organization to react to them?
D	Phishing	• To counter email and social media attacks, **what portion of the organization reflects training?** How does the organization **report attacks**?
E	SSL Everywhere	• How **secure are our communications** across networks, both within the organization, and with sanctioned cloud services?
F	Insurance Coverage	• In the event of a breach, **do we have appropriate coverage to mitigate costs**, with contingency funds and **access to specialist resources**?
G	New Printers	• How does the organization **manage infrastructure, endpoint management and privileged account access** using printers as a proxy?
H	Communications	• What are the **roles and policies that have or are yet to be defined**, as well as the **quality and usefulness of what is currently communicated**?
I	Unsanctioned Cloud	• What are the **incidences and controls on unsanctioned technologies**? How do they reflect more broadly **cloud and other addition procedures**?
J	Guest WIFI	• How is **network access granted? Guest WIFI managed?** Both are proxies for basic intranet and internet security …

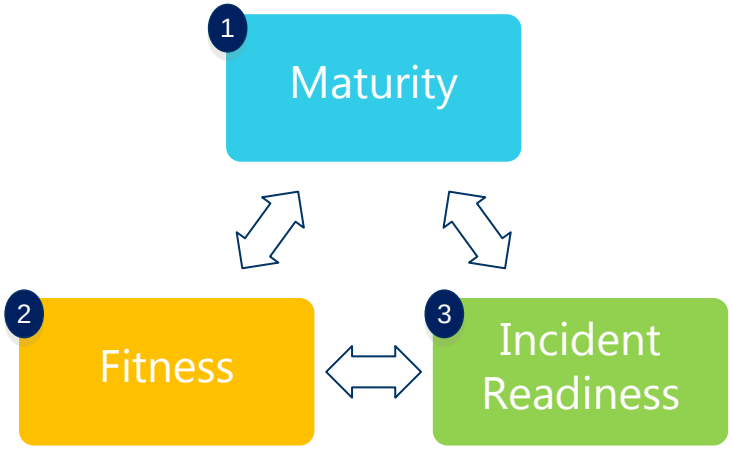


Translates to 3 Evaluations

1. Maturity
2. Fitness
3. Incident Readiness

3 ACTION AREAS - HPA CYBERSECURITY DIAGNOSTIC

The diagnostic provides detailed analyses coupled with action plans and a change program to close identified gaps in the three evaluation areas



Complex, Full Assessment (NIST)

This model simplifies communication with the organization and can be used as the basis for three independent change programs. Specific findings and recommendations can also be mapped onto NIST CSF

1 Maturity

- The maturity of an organization is measured in context and shows **how well developed its cybersecurity controls are**
- Use of controls that are overly complex or inappropriate in one environment can be as detrimental as they are effective in the right
- **Controls must therefore be right sized** and appropriate for the organization's industry

2 Fitness

- The fitness of an organization determines **how well it is able to protect itself and deal with detection** of new threats
- A fit organization is **able to automate the mundane and quickly identify exceptions** that require valuable and often scare resources

3 Incident Readiness

- Incident Readiness measures **how comprehensive mitigation plans are, how well processes are rehearsed and the mechanisms that exist are to learn from experience**
- Every organization needs to be in a constant state of Incident Readiness and ready to deal with both the background load of routine incidents as well as prepared for the next big one

HPA

HPA SENIOR ADVISORS: TECH. AND CYBSECURITY

ROXANE DIVOL

Roxane leads HPA's Technology Strategy efforts with over 20 years of experience as a senior technology executive and management consultant. She has advised companies across strategy, growth, organizational structure, operational improvement, and go-to-market optimization.

She currently serves as a Board Director of Wolverine Worldwide, a multi-billion dollar global footwear provider, where she also sits on the Audit and Governance Committees.

From 2013 to 2018, Roxane was a senior executive (and HPA client) with Symantec. Most recently she was EVP and GM of its Website security business - which was successfully sold to a private equity firm; as well as Executive Sponsor and founder of its CyberCube Analytics business, which has now been launched as an independent start-up.

From 1996-2013, Roxane worked with McKinsey, where she was a Partner in the firm's San Francisco office. Her client work focused on topics ranging from strategy to go-to-market and organization, including multinational technology firms. Roxane also created a senior executive roundtable for women, of which she is still a part.

Roxane graduated from France's leading engineering academy, Ecole Polytechnique, and obtained an MBA with distinction from Insead.

BOB KAPLAN

Bob leads HPA's IT and Systems Practice with over 35 years of experience as a senior executive and management consultant. He has deep expertise in the areas of strategy development and implementation, organizational effectiveness, and information systems and technology.

Bob spent 12 years at BCG, where he was Managing Partner of the San Francisco office before joining McKinsey as a Senior Partner in their North American Technology and Systems Practice, which he led for 10 years.

After leaving McKinsey, Bob served as CIO for Silicon Valley Bank; and on the Boards of Alibris, an ecommerce company; Greater Bay Bancorp, a regional bank acquired by Wells Fargo; ITM Software, a software and IT company; and is currently serving as a Board Member to Lanetix, a 3PL software provider; and Motif, an outsourcing service provider.

Additionally, Bob served on the Technology Advisory Peer Group for the State of California, acting as an advisor to the state CIO.

Bob received his MBA from the Stanford Graduate School of Business. He also completed all requirements, except dissertation, for a PhD in computers and information systems, also at Stanford. He graduated with exceptional distinction in Economics from Yale University.

HPA

HPA SUBJECT MATTER EXPERTS AND LEADS (EXAMPLES)

SEAN D.

Sean is a senior executive and consultant focused on cyber and information security with over 25 years experience spanning a wide range of verticals. Sean works with C-level executives at both technology and services companies, as well as end-user and industry organizations to create solutions that address the ever evolving threat landscape and security constraints.

PROFESSIONAL BACKGROUND

- 1 year – Consultant focused on tech. and information security initiatives across industries
- 11 years – Multiple executive roles, Symantec, including Vice President, Technology Partnerships and Alliances; VP, Technical Strategy and Operations; VP and CTO Enterprise Security; and Senior Director, EMEA Security Business Practice and NNE Business
- 1 year – Technical Director, Imlogic
- 1 year – Marketing Director, Lenton
- 14 years – Multiple positions, RCMS; worked through company from Intern to Group CTO
- BS, University of Surrey

CASE EXAMPLES

- Act as Strategic Advisor to Tala Security to help websites and web apps enable a complete, secure web experience for users by protecting from a variety of client-side attacks including XSS, cryptojacking, clickjacking and ad injections. Currently working with major financial services and retail companies to eliminate Magecart attacks
- Act as Strategic Advisor to Centraya, the European cloud access security broker built to meet the highest requirements for data privacy in any cloud application
- As VP, CTO Enterprise Security for Symantec, reported to EVP Enterprise Security and focused on driving initiatives to support the CISO community globally. Efforts included the development of blueprints for specific technologies and security services offerings
- As VP Technology Partnerships and Alliances, worked with vendors including Cisco, VMware, Intel, Palo Alto Networks, Splunk, zScaler, and Fortinet to collaborate on product and service integrations to create solutions around technologies, including micro segmentation in software-defined networks and scalable data loss protection
- Provided executive and subject matter expertise to Global 2000 customers post-breach with a focus on better deploying/configuring existing technology to increase protection
- Founded an alliance on behalf of shared customers between cybersecurity vendors (Symantec, McAfee, Palo Alto Networks, and others) to enable the timely sharing of incident intelligence
- For a Fortune 500 technology organization, created a process to streamline and increase accuracy of the technical and security due diligence process for investments and inbound technology licensing
- Act as frequent guest speaker and contributor at multiple major international security conferences and events

KERRY G.

Kerry has over 25 years of experience in the software and information technology sectors, and has expertise in solving business problems in both technology and management consulting capacities. He has both driven development of strategy and led implementation initiatives for companies across industry sectors.

PROFESSIONAL BACKGROUND

- 17 years – Consultant and business leader focused on information technology initiatives
- 3 years – President, International Association of Microsoft Channel Partners-US, a not for profit organization focused on enabling companies to increase partnering and best practices
- 5 years – CEO/President, Horizon Software Development, ISV focused on document management
- 1 year – Technology Research Analyst, Morgan Guaranty Bank
- 2 years – Technology Analyst/Officer, Citibank
- BA, SUNY-Binghamton

CASE EXAMPLES

- As part of a larger, long-term IT strategy effort for a $2B healthcare services organization, acted as Head of Infrastructure driving cloud migration to better cyber/information security in accordance with HIPAA. Worked closely with CISO to secure Microsoft Business Associate Agreement to assure coverage in case of loss of protected health information
- For a FINRA-certified international issuer of government bonds with operations in the USA, Canada, and Latin America, assisted in the development and implementation of new cybersecurity roadmap. Efforts included:
  - Implemented CyberArk, a Privileged Account Security system to enhance transparency and log of administrator actions
  - Implemented web application protection to harden public, consumer facing website against access/attack from suspect regions/IP addresses
  - Acted as lead on build-out of cloud-based international strategy. Tasked with mapping company's first international cyber strategy to US security plan
- Led implementation of a system designed to maximize the cash flow for hospitals through the reduction of insurance company rejections by providing quick and automated responses to denied claims based on the specific explanation of benefits
- Assisted a quasi-governmental organization to align their business objectives with the creation of an online bond purchasing system that has exceeded the customer's expectation in driving net new business. Provided additional services to integrate all sales and customer service actives with a newly developed CRM system
- Helped a worldwide retailer to create a Services Oriented Architecture (SOA) that supports key business objectives including the ability to more easily integrate and sell off online retail properties. Integrated new search technologies and strategies to reduce the number of page views per purchase leading to increased revenue

WHY HPA?

Engagement	HPA engages clients with a focus on understanding the why before executing the how. HPA engagements only begin after in-depth discussions between Partners, Senior Advisors, and Client Executives around the core issues that need to be addressed
Experience	We hand select teams with relevant operating, technical, ***and*** top-tier consulting experience, a unique blend that enables us to craft practical solutions based on real world experience, not simply presentations or ideas
Collaboration	We believe that breakthrough ideas come from combining our knowledge and experience with yours – when client and HPA team members discover solutions together, the result is high value solutions that get implemented
Flexibility	We are not “one-size-fits-all” where every team is structured the same way, regardless of client individual needs, size, and capacity. We also have the ability to flex our involvement as work progresses – heavier involvement in earlier stages, and lighter involvement as we move into client ownership of programs

CASE STUDIES (1 OF 2)

Client

Publicly Traded SaaS Provider

Project

Cybersecurity Evaluation during Acquisition Diligence

Diagnostic was deployed on a regular basis as a means for evaluating a target company's cybersecurity fitness during the M&A due diligence process.

On two separate occasions, results of the diagnostic were used as the determining go/no-go acquisition factor for the parent organization. The first found the target company incompetent in most cybersecurity areas resulting in an exposure risk too high for the acquiring company and termination of the deal. The second found the company to have operationalized the detection and response to threats / incidents resulting in a mature cybersecurity organization allowing the acquisition to proceed.

Client

Pharmaceutical Company

Project

Firm-wide Cybersecurity Evaluation

Deployment of the diagnostic lead to the identification of significant differences in phishing rates, a lack of understanding on incident detection, and significant inconsistencies in the proper use of VPN, WIFI, and physical network procedures between the company's headquarters and regional offices.

Findings resulted in the development of a strategy where regional offices are now treated as untrusted environments requiring the use of a secure guest network, and employees connecting via VPN now use software tokens build into their phones and tablets. Driven by employee demand, the company adopted the strategy at their headquarters along with extensive cybersecurity education

CASE STUDIES (2 OF 2)

Client

Fast-Moving CPG company

Project

Legacy Systems and Practices Gap Identification

Following a significant investment in cybersecurity, including attainment of ISO27001 certification, client deployed the diagnostic which identified issues with legacy systems and practices, basic training gaps for individual contributors, and executives who did not have an understanding, or were unaware of, their role during a major cybersecurity incident.

The diagnostic was used to guide the client to close these and other gaps and continue to strengthen their posture. As a result, the organization has been successful in defending against and reacting to a number of significant attacks against them.

Client

Regional Hospital System

Project

Cybersecurity Evaluation during Partnership Evaluation

Diagnostic was used by a third-party to determine the maturity, fitness, and incident readiness of an organization during diligence for a potential partnership. Findings highlighted issues with the management and communication of malware throughout the company. Despite significant investment in detection technologies at the endpoint, network, and email gateways, they had no automation or repeatable processes established.

The third-party client presented management with diagnostic findings, which they agreed with but were slow to act upon. Approx. 18 months later, the organization had a serious Ransomware infection resulting in a third of all machines requiring re-imaging.

HPA | HighPoint Associates

CONTACT US

West Coast
100 N. Pacific Coast Highway
Suite 620
El Segundo, CA 90245
310-616-0100

East Coast
641 Lexington Ave.
15th Floor
New York, NY 10022
212-634-6496

Sumeet Goel
Founder and Managing Director
sgoel@highpoint-associates.com

Richard Berger
Partner
rberger@highpoint-associates.com

Justin Moser
Chief Operating Officer
jmoser@highpoint-associates.com

highpoint-associates.com