HIGHPOINT

MANAGING RISK THROUGH CYBER SECURITY MEASUREMENT

REDUCING RISK EXPOSURE

Requires the ability to firstly measure this risk

According to Gartner, organizations worldwide will spend $170.4 billion on protecting their business from ever increasing cyber security threats. However, despite increasing your spend on cyber security, it only takes one vulnerability to expose your organization to a critically-damaging attack.

The challenge is making the right investment appropriate to your risk and more importantly, making these investments in the right place. Unlike with other investments, most organizations spend on security without truly evidencing the risk they are mitigating and the return on investment.

HighPoint helps you to break this cycle. We enable you to understand where the most critical risks are across your business and to measure these risks in order to invest appropriately in the right areas.

Our approach to Cybersecurity Measurement is designed to help you to understand your risk exposure and to determine the effectiveness of current and future investments in security.

It answers key questions such as:

- Where are my greatest cybersecurity risks?
- How effective are my current controls in protecting sensitive data?
- What gaps/vulnerabilities exist across people, processes and technology related to cybersecurity?
- How are my people, processes and technology working together to reduce risk and likelihood of compromise?

CYBERSECURITY MEASUREMENT

Our holistic approach to measuring risk & security effectiveness

According to Accenture, over two-thirds (68%) of business leaders feel that their cybersecurity risks are increasing. The keyword here is ‘feel’ rather than ‘know’ and this is due to the lack of measurement of risk.

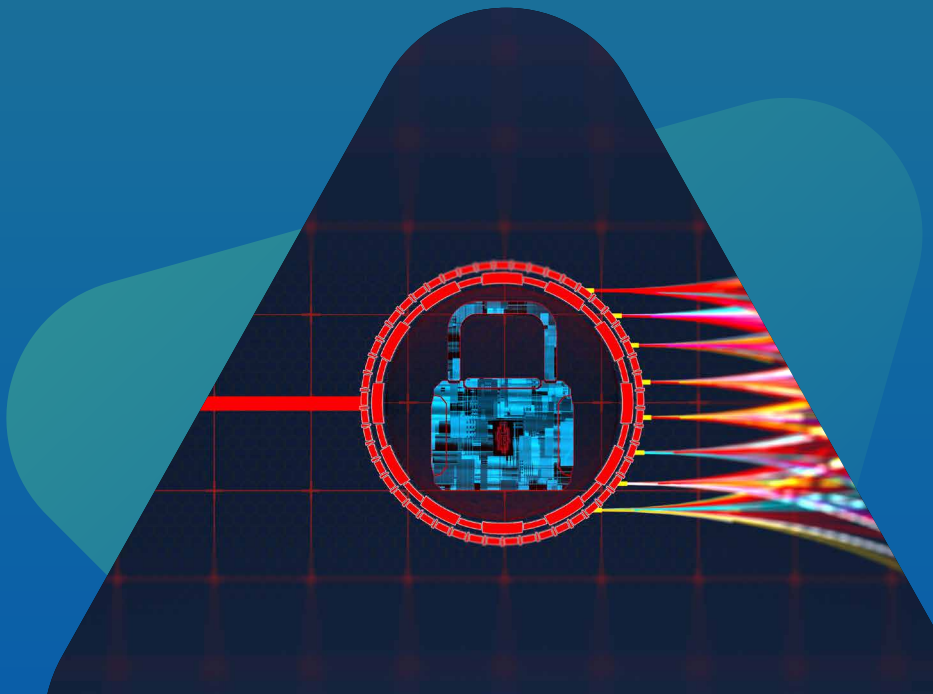
Investment is often driven on the fear of potential exposure. Stats such as those from IBM that estimates the average cost of a data breach is now $3.86m and the average lifecycle of a breach is 280 days. However, no two businesses are the same and unless you understand your holistic security posture it is difficult to invest in the right areas at the appropriate level.

HighPoint takes a holistic approach, firstly taking the time to understand your business and the impact and consequences of a cyber attack or data breach. With this understanding we are then able to assess and measure your risk and cyber security effectiveness.

This holistic approach takes into account your security policies and processes and measures these against best practices to identify gaps and potential areas of weakness.

We then meticulously review your technology infrastructure and how this is being protected and managed to reduce cybersecurity threats and measuring the effectiveness of what you currently have in place.

Finally, we focus on your people. According to Cybint, 95% of cybersecurity breaches are caused by human error. We gauge the security awareness of your people and measure the risk and exposure from the way they work.




The average ransomware payment is rising at a rate of **33%** year on year
Source: Fintech News
On average, every employee has access to **11 million** files.
Source: Varonis
1 in 13 web requests lead to malware.
Source: Symantec
Since the start of the Covid Pandemic, the FBI reported a **300%** increase in reported cybercrimes.
Source: IMC Group
By 2023, the total number of DDoS attacks worldwide will be **15.4 million**
Source: Cisco

INTERNET PERIMETER REVIEW

Assessing & measuring your existing perimeter security

Securing your perimeter is critical in protecting against cyberattacks and unauthorized access. However, today the perimeter is no longer well defined. Digitalization is driving more people and things being connected to your environment, and this infrastructure spans hybrid cloud and platforms that you no longer own.

Perimeter Architectural Review

We help you define your actual perimeter and the common internet-facing services you have in place such as web services, FTP gateways, email servers and remote access technologies. We assess how your network is segmented to logically separate these access points from internal systems.

We review the technologies you have in place such as Firewalls, Web Gateways and Intrusion Detection/Prevention Systems and measure the effectiveness of this in detecting, responding and remediating risk.

Perimeter Console Review

The effectiveness of your perimeter security is not just measured in terms of the technologies you have in place, but how these are configured and managed to reduce risk.

We take the time to comprehensively assess the configuration of your security appliances and applications ensuring a hardened configuration is in place to mitigate unnecessary risk. As part of this review, we drill into key areas such as firewall configuration files, TCP/UDP services running on exposed systems and overall system lockdown status.

INTERNAL ARCHITECTURE REVIEW & VULNERABILITIES SCANNING

Measuring architectural risk & identifying areas of risk

Cybersecurity is not just an external threat; many data breaches and malicious activity originates from inside an organization's perimeter and as such, it is important that you are able to measure internal risk and vulnerabilities.

Internal Architecture Review

We assess how your internal IT Infrastructure has been architected with a particular focus on your LAN, WAN and Wireless networks. We drill down on your layer 2/3 network segmentation, system and circuit redundancy and wireless security parameters.

Internal Console Review

The console review looks to measure the steps taken to configure your infrastructure to create a secure environment. We assess the configuration of your switches, routers, wireless network and servers and ensure that all systems have been locked down. We also review your Active Directory global policy security parameters as well as identifying and assessing every device that is connected to your internal network.

External & Internal Vulnerability Scanning

This plays a critical role in enabling you to understand and measure both the internal and external vulnerabilities that exists across your IT infrastructure.

Externally we identify the risks associated with open ports and potential application vulnerabilities exposed to the public internet. Internally we assess all devices connected to your network to identify open ports and vulnerable/unpatched end-user devices and servers.

With an estimated two-thirds of cyber-attacks exploiting vulnerabilities where a patch is available and not yet deployed, this is a critical part of cybersecurity measuring and risk reduction.

PENETRATION TESTING

Measuring system & process risk

As part of our holistic approach to Cybersecurity Measurement, we do not just assess your IT infrastructure and the security measures you have in place, we also look at how easy it is to bypass these and penetrate your environment.

With our Penetration Testing services, HighPoint seeks to actively compromise potential vulnerabilities to gauge and measure your exposure to risk. We do this in a number of ways that tests both your systems, policies and processes.

External White Hat Hacking

The aim of this exercise is to measure your risk exposure from someone external to your organization to exploit internet-facing vulnerabilities. The test of the white hat hacking is to gain unauthorized access to any system whether it be internet-facing or gaining internal system access through a compromised external system.

This process is conducted from an external system over the public internet by experienced ethical hackers.

Internal Console Review

Our penetration testing also covers the potential vulnerabilities that exist on your internal network. This aims to simulate an employee or a guest gaining access to your internal network and using this to gain access to systems, applications and data that should be restricted.

We do this by placing a laptop on your internal network and then utilizing our white hat hacker to discover and exploit vulnerabilities within your internal infrastructure.

PENETRATION TESTING

Measuring the risk associated with your people

This part of our penetration testing focuses on assessing the security awareness and behaviors of your people to measure the risk associated with this. We do this by looking to penetrate your environment through your people and your physical locations.

Social Engineering (Remote)

Social engineering looks to assess the ability, and therefore the risk, to gain confidential information or system access through the use of your people and is a proven way of measuring security awareness across your organization.

We utilize many approaches to this including phishing emails, phone calls and social media interaction. Our average response rate of being able to collect Windows user credentials is 12% through phishing emails alone.

When this is combined with our white hat hacking, HighPoint is often able to gain access to key systems such as email and collect a wide range of sensitive information.

Social Engineering (Onsite)

Securing your facilities is a key part of Information Security and failing to do this can provide access to internal systems and vulnerabilities that can exploited.

This part of our penetration testing aims to gain unauthorized access to your property utilizing a wide range of tactics to get through locked doors and pass-through security and reception. Once we have been able to access your physical premises, we use a number of techniques to gain access to sensitive information ranging from finding usernames and passwords on desks, information in trash bins, connecting to an access-point to the network and even connecting phone home devices.

WEB APPLICATION ASSESSMENT

Measuring the cybersecurity of your digital world

As we accelerate digitalization, we now utilize a plethora of web applications to provide business-critical applications to end-users and digital interfaces to our partners, customers and suppliers.

The nature of web applications is that they utilize ports 80 and 443 which have traditionally been blocked by firewalls and as such opens up exposure to an extended attack area. In addition to this, web applications leverage a wide range of APIs to interoperate and share information all of which adds to potential vulnerabilities.

Our Web Application Assessment looks to understand how these applications have been coded and interoperate in order to identify areas of risk and measure the associated cybersecurity threats.

Our approach to Cybersecurity Measurement is designed to help you to understand your risk exposure and to determine the effectiveness of current and future investments in security.

We focus on understanding your vulnerability and potential risk from the common attack vectors associated with web applications including:

- Cross-site scripting.
- SQL injection.
- Brocken authentication.
- Security misconfiguration.
- Missing function-level access control.
- Cross-site request forgery.
- Known vulnerable components.
- Unvalidated redirects and forwards.

CIS TOP 18 ASSESSMENTS

Evaluating your risk across the 18 critical security controls

There are many security standards and compliance requirements with a high degree of overlap of what they cover. Applying all of these is simply not possible and knowing which one is best is a challenge.

In response to this challenge, the Center for Internet Security (CIS) coordinated the development of the ’18 Critical Security Controls (CSCs) for Effective Cyber Defense’ which is what we follow at HighPoint.

This list of controls was developed in conjunction with a number of government departments and private industry experts and represents the general consensus on the most practical and effective security controls to significantly reduce an organization’s security risk.

The US State Department has stated that they have observed a 94% reduction in measurable security risk through the rigorous application of the CIS Top 18 security controls and this is why we focus on these areas.

As part of this assessment, we interview key stakeholders across your organization in order to assess and measure your security against these 18 critical security controls.

This enables us to determine how you stack up against these critical areas and provide you with a detailed list of recommendations that will enable you to reduce cybersecurity risk.

THE VALUE WE DELIVER

By assessing & measuring your cybersecurity risk

HighPoint combines deep-rooted experience with a highly methodical approach to measuring cybersecurity. We believe this delivers significant value to our clients in being able to understand, measure and address the cybersecurity risk to their business.

We enable you to take a holistic prospective to cyber security that considers not just the technology components you have in place, but also how your processes expose you to risk and the security awareness of your people.

The threat that is faced by every business will not go away and will only increase as cyber criminals become increasingly sophisticated and persistent in their approaches. Organizations need to recognize that they will be attacked and some of these attacks will result in a breach and therefore they need a thorough approach in place to quickly identify, remediate and recover from such breaches.

Visibility of risk

We provide you with the important visibility into the risk your business faces from cyber-attacks. We help you measure this risk in order to be able to take the appropriate level of action.

Informed Investment

We identify those areas that poses the greatest risk to your business and as such enables you to make informed decisions. You understand the gaps in your security posture and the measurable return on each investment in securing your organization.

Reduced & Managed Risk

By prioritizing your security investment in those areas that pose the greatest level of risk and remediating vulnerabilities that were previously unknown you take a significant step to reducing and managing the cybersecurity risk.

www.highpoint.com

HIGHPOINT