8 CRITICAL CONTROLS FOR CYBERSECURITY AND INSURANCE COVERAGE

As our world becomes increasingly digitized, we see increasing opportunities for innovation and improvement. But with every advancement, new vulnerabilities emerge, casting shadows over our progress. For businesses, the reality of cybersecurity breaches isn't a question of 'if' but 'when'. From data leaks that can tarnish a brand's reputation overnight to cyber attacks that can cripple entire operational frameworks, the threats are vast. Even more concerning? The rapidly changing nature of these threats makes yesterday's defense mechanisms obsolete today.

Enter Arch CyPro's 8 Critical Controls: a 360° shield in this volatile cyber landscape. But how can businesses integrate these controls seamlessly? And why are they pivotal in securing not just your digital assets but also your insurance coverage?

8 Critical Controls for Cybersecurity and Insurance Coverage

By Kyle Lutterman

In the digital age, where businesses are embracing technology at an unprecedented rate, the need for robust cybersecurity has never been greater. Data breaches, cyberattacks and phishing schemes have surged in recent years, putting countless businesses and their reputations on the line. In fact, according to a recent report from Zscaler, observed phishing attacks increased by a staggering 47.2% in 2022 compared to the previous year.

Yet, while threats continue to grow and diversify, so too do the measures and strategies to combat them. That's where Arch CyPro's 8 Critical Controls come into play.

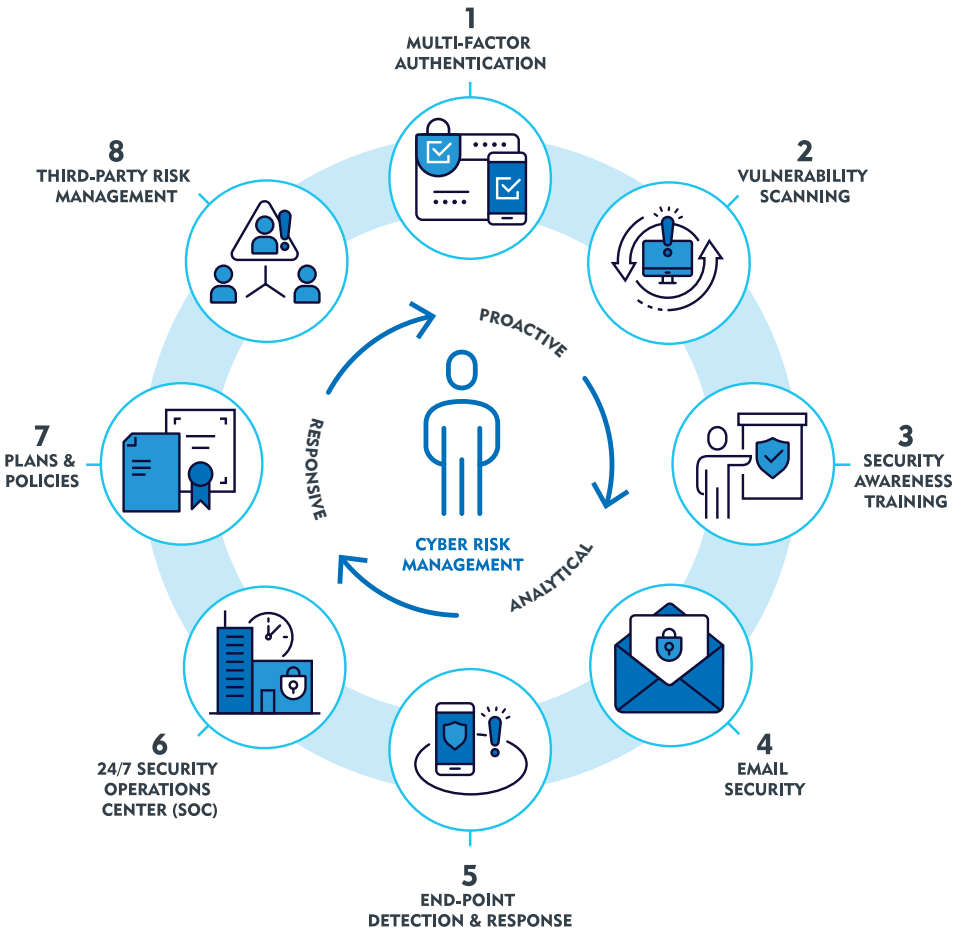
Acting as cybersecurity guidelines, these are essential pillars that help organizations safeguard their digital infrastructure, protect sensitive data and maintain business continuity. Implementing these controls not only strengthens an organization's cyber resilience but may also make it more attractive in the eyes of insurers, leading to better coverage options and terms.

By understanding and integrating these controls, businesses can navigate digital complexities with confidence and secure their futures - online and off.

ARCH CYPRO'S 8 CRITICAL CONTROLS

Arch CyPro's 8 Critical Controls represent a holistic approach to cybersecurity, addressing a broad spectrum of vulnerabilities that organizations may encounter. These controls, categorized into **proactive**, **analytical** and **responsive**, provide a structured approach to tackling cyber challenges, ensuring protection as well as adaptability and resilience.

But what truly sets these controls apart is their comprehensive nature. Instead of addressing just a single issue, each control fortifies an entire facet of an organization's cyber posture.



Arch | Insurance

PROACTIVE CONTROLS

According to the Verizon DBIR, stolen credentials, phishing and exploitation of vulnerabilities are the top three methods attackers use to infiltrate organizations. Proactive controls tackle these head-on, serving as the first line of defense. They encompass:

Multi-Factor Authentication (MFA): An added layer of security, requiring multiple forms of verification.

Vulnerability Scanning: Regular checks to detect and address weaknesses in a system.

Security Awareness Training: Equipping employees with the knowledge to recognize and mitigate threats.

Together, these proactive controls reduce the risk of unauthorized access and data breaches by deterring potential threats before they materialize.

ANALYTICAL CONTROLS

Vigilance in cybersecurity cannot be understated. Analytical controls act as the eyes and ears of an organization's cyber defenses, constantly on the lookout for anomalies and potential threats.

A startling fact from Sophos Incident Response reveals that over 90% of ransomware attacks occur outside typical working hours. With the correct analytical controls in place, businesses ensure round-the-clock surveillance and immediate response to threats, even when the regular workforce is offline. These are:

Email Security: Advanced filtering and detection mechanisms to defend against malicious, email-borne threats.

End-point Detection and Response (EDR): Monitoring and addressing threats at individual device levels.

24/7 Security Operation Center (SOC): Offering round-the-clock surveillance, ensuring threats are detected even outside of typical working hours.

OVER **90%**

OF RANSOMWARE ATTACKS OCCUR OUTSIDE OF BUSINESS HOURS (8AM-6PM, MON-FRI)

RESPONSIVE CONTROLS

In the unfortunate event of a breach or cyberattack, how an organization responds can make all the difference. Responsive controls are these action plans, ready to be deployed at a moment's notice. The two key components here are:

Plans & Policies: Prepared action blueprints for different types of cyber incidents.

Third-Party Risk Management: Strategies to ensure external partners and suppliers maintain cyber hygiene, preventing them from becoming exploitable weak links.

A recent Black Kite report found that only 34% of organizations are confident in their suppliers' or primary third parties' willingness to notify them about breaches. Responsive controls prepare organizations for such contingencies, ensuring rapid containment of threats and minimizing potential damage.

These eight controls, each essential in its own right, form a cohesive, comprehensive strategy when combined. They arm organizations with the tools, strategies and methodologies to respond to the cyber landscape of today and be prepared for the uncertainties of tomorrow.

WHY THESE CONTROLS MATTER FOR INSURANCE COVERAGE

The strength and resilience of an organization's cyber defenses are pivotal when it comes to cyber insurance. Embracing Arch CyPro's 8 Critical Controls underscores an organization's commitment to cybersecurity and diligence in reducing its risk profile. This preemptive approach has two significant benefits.

Firstly, insurance providers recognize the lowered threat of potential claims and, in many cases, offer reduced premiums as a reflection of this decreased risk. Secondly, as cyber threats diversify and become more sophisticated, the insurance industry continually expands its coverage offerings. Organizations strategically implementing these controls can access a more comprehensive and tailored set of coverage options, ensuring they're shielded against even the most unforeseen cyber events.

The controls themselves have been identified by the Arch CyPro team, through decades of experience in cyber underwriting. They're the checklist used to help us assess incoming risk, support the claims process and constantly learn from cyber breaches to ensure businesses remain resilient.

In short, these controls not only fortify an organization against cyber threats but also position it advantageously within the insurance landscape.

Implementation Guidance

Step 1:

Assess Current Maturity

Robust cybersecurity begins with a thorough assessment of the current state of each of the Arch CyPro 8 Critical Controls within your organization. This evaluation is crucial to determine not just the existence of these controls but also their maturity level and how well they are integrated into your wider systems.

A key focus area for a defense-in-depth strategy is Multi-Factor Authentication (MFA). For all email and remote access, MFA acts as the first critical barrier to prevent unauthorized access and safeguard sensitive information. Understanding where your organization stands with each control will set a clear baseline for improvement.

Step 2:

Develop a 60-Day Implementation Plan

Once the current state is understood, the next step is to develop a comprehensive 60-day implementation plan. This plan should detail the steps needed for either the implementation of new controls or the enhancement of existing ones. It should ideally consist of:

- An **assessment phase**, using the findings from step 1 to highlight any existing gaps in your cybersecurity practices.
- A **training phase** to educate staff on their roles in the cybersecurity framework and the importance of practices like MFA.

Collaboration with your broker or insurance provider is vital during this stage. They can offer valuable insights into how your plan aligns with insurance coverage requirements, ensuring that you not only enhance your cybersecurity posture but also remain compliant with insurance standards.

Step 3:

Partner with Key Suppliers

In the implementation or enhancement of these controls, partnering with key suppliers is a strategic move. Arch's solution-focused approach includes strong relationships with leading suppliers in cybersecurity. By leveraging these relationships, policyholders can streamline the implementation process, accessing cutting-edge tools and resources from our carefully selected panel.

Your organization's cybersecurity strategy deserves the meticulousness and foresight that Arch CyPro's 8 Critical Controls offer. If you're ready to strengthen your cyber resilience or want to learn more about these controls, Arch is here to guide and support. Visit our website at **archinsurance.com/cypro** for comprehensive resources, or reach out to our team of experts for tailored assistance.

Author

Kyle Lutterman is an Information Security Professional with over 10 years of experience in managed services with a focus on incident response. He has supported multiple government agencies and Fortune 500 clients and currently leads the Cyber Risk Engineering team at Arch Insurance. In this role, he developed a proprietary framework for cyber insurance underwriters to follow and he consults with organizations seeking to enhance their cyber controls to obtain cyber insurance. In his free time, Kyle enjoys golf and playing with his two young children.

Arch CyPro

Arch Insurance has long been a force and a recognized global leader in the cyber insurance industry, protecting the critical operations of digital businesses. Now, with its new cyber insurance offering, CyPro, Arch is taking a proactive approach to protect its insureds from the ever-evolving threat of cybercrime.

Arch Insurance

Arch Insurance is a market-leading insurer, providing a wide range of property, casualty and specialty insurance options for corporations, professional firms and financial institutions across the U.S. Our approach to doing business is based on collaboration, responsiveness and commitment. Together with our business partners, we pursue better ways of doing things and designing more effective solutions to respond to the needs of our customers.

Scan the code.
Discover more.

Pursuing Better Together®

archinsurance.com/cypro