EBOOK

Cybersecurity Game Plan for Cyber Insurance Before You Buy, Negotiate or Renew

ordr

State of Cyber Insurance

Feeling stung by the increased premiums insurance providers are requiring for cybersecurity coverage? You're not alone.

The bad news:

Policies are more expensive than in recent years and insurance providers are limiting their coverage and payouts.

The good news:

There are actions you can take as a CISO and security leader to defend your organization against attacks and not only qualify for a cyber insurance policy, but improve your negotiating position.

This paper will guide you on creating a game plan before you buy, negotiate, or renew your cyber insurance policy. You'll gain insight to the 12 distinct security controls recommended by a leading cyber insurance firm, and guidance on how Ordr can help meet conditions required for obtaining coverage while also going a step beyond to ensure maximal security and the best premium price available.

Why the Increase

Prices for cyber insurance policies rose more than 100 percent year-on-year by the end of 2021, then moderated to 79 percent in the second quarter of 2022 and 48 percent in the third, according to Marsh McLennan, one of the leading insurance underwriters in the United States[1]. This was due in part to policies being underpriced for several years, causing insurers to take losses in 2018 and 2019 as claims mounted. But as we noted in our The Rise of Cybercrime report, a confluence of widely available ransomware attack tools, cryptocurrency, and cybersecurity insurance itself drove this escalation, with damages increasing tenfold between 2016 and 2020.

Today, the shock of price increases and complexity of applying for insurance, plus the exclusions on coverage that some insurers are putting in place, are causing many organizations to rethink the value of insurance.[2] Buyers don't have much room to maneuver. The cybersecurity insurance industry is concentrated in only 10 providers[3], compared to more than 700 providers selling life insurance[4] and 5,000 selling auto insurance.[5] And those 10 providers now require their customers to prove they have adopted certain security measures before they'll issue a policy. In one high-profile case, Travelers Insurance successfully defended its refusal to pay a claim because the insured organization had misrepresented its technical preparedness for attacks.[6]

Indeed, some industry segments are being shut out by insurers altogether. The U.S. General Accounting Office (GAO) noted that some carriers are limiting the coverage they'll provide to certain critical infrastructure sectors. Said a GAO representative, "One insurer reported that it opted not to insure the energy sector because of its vulnerability to attacks and because of concerns that energy operators do not follow robust cyber security protocols."[7]

[1] *"Rising cost of cyber attacks sends insurance policy charges soaring," by Oliver Ralph, Financial Times, Nov. 8, 2022 (https://www.ft.com/content/753e76db-e9cc-4c90-985a-f354dbc5c9a4)*

[2] *Financial Times*

[3] *S&P Global Market Intelligence*

[4] *https://www.statistica.com/statistics/194335/total-number-of-life-insurance-companies-in-the-us*

[5] *https://wallethub.com/answers/ci/how-many-car-insurance-companies-are-there-2140804128/*

[6] *"Travelers, Policy Holder Agree to Void Current Cyber Policy," Chad Hemengway, Insurance Journal, Aug. 30, 2022*

[7] *"Rising premiums, more restricted cyber insurance coverage poses big risk for companies," Bob Violino, CNBC, Oct. 11, 2022*

Due to greater risk exposure across the cyber insurance market, an increase in underwriting scrutiny is here to stay and will only increase exponentially over time as the market matures. This trend may also be exacerbated by external strains on the global financial services industry and any negative macroeconomic and geopolitical influences that ripple across all industries. That includes an escalation in cyber warfare between state actors in an increasingly digital world.

In areas of high geopolitical tension, there has been a reported growth in the number of state-targeted cyber attacks. Petya and NotPetya attacks, first discovered in 2016, were a turning point for "silent cyber" exposure[8] and exclusions for acts of war. NotPetya attacks led to lawsuits like Mondelez v. Zurich and Merck v. Ace as companies fought their insurance provider over what they felt should have been covered, but was not explicitly outlined as covered, with affirmative language within their policies. In early 2022, Lloyd's Market Association (LMA) began to address these concerns by publishing four cyber war exclusions[9]. The release of these clauses have caused concern in the cyber insurance industry and as well as added significant confusion. (Note that In May 2023 Merck prevailed in its $1.4 billion appeal of an earlier ruling that war exclusions applied to a cyberattack it suffered.[10])

[8] *https://www.marsh.com/uk/services/cyber-risk/products/silent-cyber-how-you-can-cover-perils.html*

[9] *https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx*

[10] *https://www.insurancejournal.com/news/east/2023/05/02/718771.htm*

Benefits of Cyber Insurance Drive Adoption Despite Rising Costs

Even so, more and more organizations are applying for cyber insurance as part of a balanced risk management portfolio. Lloyd's of London estimates that the global cyber insurance market will rise from $12 billion of annual premiums in 2022 to more than $60 billion in the next five to 10 years as threats increase.[11] That increase may be due because providers recognize the benefits extend beyond financial compensation for losses. Insurance providers have experts on staff who can help their clients negotiate when cybercriminals demand exorbitant ransomware payments, for example. Because these experts have been through these high-stress situations before, they can take a more measured approach than a CISO who has never faced an extortion threat.

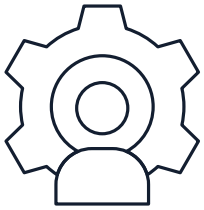
Despite the rising costs, stricter qualification requirements, and policy limitations, more companies are opting to get cyber insurance. For one, it transfers some (not all) of the financial risk associated with a successful cyber attack. It also has indirect benefits that outweigh a policy's direct cost by raising the bar for organizations to implement more strict cybersecurity policies and best practices, as well as offsetting and buffering complex litigious business environments. And finally, cyber insurance has become a non-negotiable cost of doing business as more third parties are increasingly requiring coverage as a precondition for doing business.

[11] *Financial Times*

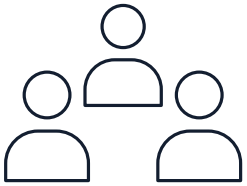
Adjusting to the New Insurance Reality

Given the complexities and dynamic nature of the cyber insurance market, and increasingly stringent security controls underwriters require of their customers, CISOs now play a significant role in helping their organizations to get the coverage they need, and at the best possible price.

Specifically a CISO has two vital roles to play in this process:



Meet with other executives and managers in the organization to determine how to assess the level and type of coverage that is appropriate, given your organization's risk tolerance. It is also an opportunity to encourage other non-insurance measures you can take to decrease the risk and impact of cyber threats.



Work with your team to be fully prepared to answer an insurance provider's questions about organizational and technical actions your organization has taken in advance of seeking cyber coverage, and to provide documented proof of compliance with an underwriter's required controls.

Creating a Game Plan for Cyber Insurance

Attacks have become increasingly prevalent, with losses to organizations representing millions of dollars for each breach on average. Gartner predicts the financial impact of attacks targeting cyber-physical systems (CPS) will reach more than $50 billion by 2023. Other industry studies have found the average financial impact to an organization as a result of a breach is $2.8 million. In addition, nine in 10 manufacturers that have suffered a ransomware attack or breach have also had their supply chains disrupted.

As you've no doubt read before, it's not a matter of if you'll be attacked, but when. That's why improving your security posture is a good business decision. And when you do, ramping up your security level and qualifying for cyber insurance should include these steps:

Step 1: Understand Your Organization's Attack Surface and Security Posture

The first step before you buy, negotiate, or renew your cyber insurance coverage is to understand your organization's attack surface, security maturity, and risk posture. Hopefully an annual risk assessment is already part of your cybersecurity program, but consider a compromise assessment (CA), penetration test, and attack surface mapping. This allows you to baseline where you are, identify your risks, and provides guidance to embark on Step 2.

Step 2: Implement Policies and Controls to Minimize Cyber Risk

Improving your cyber risk posture and incident response readiness requires organizational planning. Engaging with all relevant parties – not just those with assigned security responsibilities but all company employees – is critical in prioritizing efforts, fending off attacks, and shutting down breaches as quickly as possible.

Next, combine your risk assessment results from Step 1 to ramping up your security level. Align to a cybersecurity framework such as NIST, or CIS Controls to ensure you are addressing all aspects of cybersecurity.

Risk reduction and reducing the enterprise attack surface is key. Whether it be blocking activity at a port, terminating a session, quarantining vulnerable devices , or proactively restricting network communications through policy - all actions are critical, and roll up to a strategic strategy to improve your organization's cybersecurity posture.

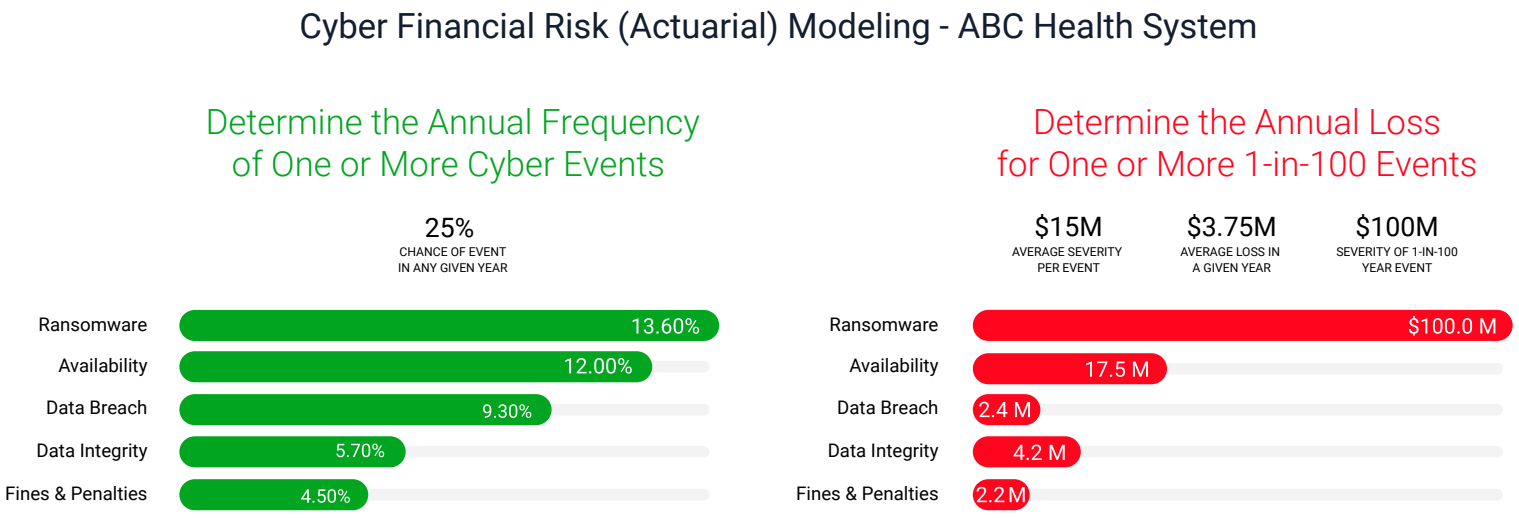
Here are some guidelines:

- Establish and maintain a current view of your organization's attack surface by discovering all devices connected to your network, including newly connected devices.
- Identify all the vulnerabilities and risks inherent in these devices.
- Take steps to remediate all identified vulnerabilities and risks.
- Apply mitigations such as compensating controls to protect remaining vulnerable devices. This can include Zero Trust segmentation policies that can restrict mission-critical and vulnerable devices to only essential, baseline network communications required for their functions.
- Employ proactive security measures to reduce the attack surface and prevent the spread of an attack.

Step 3: Map Revenue at Risk

One of the most important things an organization can do is determine the revenue impact of a cybersecurity event and map this back to cybersecurity priorities. After quantifying the risk, potential losses can be offset by establishing some fundamental cybersecurity controls defined in Step 2. You can then assess the amount of insurance coverage needed to offset these security controls, and prioritize future cybersecurity efforts to mitigate risks that cannot be covered by insurance.

For example, for a manufacturing organization, revenue at risk may be if revenue-generating production comes to a halt because of a cybersecurity incident. For a healthcare organization, it might be shutting down the hospital because of a ransomware attack. Understanding the duration of the impact, as the entire incident may take a few days or up to a week to resolve, will allow you to estimate the revenue at risk.



Model based on EOY 2022 looks at compromise probability of data breach, data integrity, availability, ransomware, and fines/penalties, and estimates for all cyber events based on 1-in-100 probability

Mitigation Strategies — What is the impact on expected losses from security improvements?

Table below highlights the initiatives currently in place to address ABC's maturity gaps, their expected impact on ABC's NIST score, and the change in expected losses.

NIST Category - Associated Projects	NIST Maturity Current (2022*)	NIST Maturity Projected (EoY 2023)	Current State Losses (2022)	Projected State Losses (EOY 2023)
Identify • MFA • PIM/PAM	2.2	2.9	Average Annual Loss: **$3.75 M** 1-in-100 loss: **$100 M**	Average Annual Loss: **$1.875 M** 1-in-100 loss: **$85 M**
Protect • Segmentation	2.1	2.7		
Detect • IOT/MIoT	2.2	2.8		
Respond • SIEM Logging • CSOC	2.5	3.0		
Recover • BCP/DR	3.0	3.1		
Overal NIST Score	**2.4**	**2.9**		

*As of End of Year 2022 Annual Risk Assessment

Step 4: Communicate with Senior Management

With the details outlined in Step 3, security leaders can now communicate with senior management and board of directors using metrics and benchmarks on how you are managing your attack surface and its associated risks, and balancing the risks with cyber insurance.

The Marsh Model: Top Cybersecurity Controls for Cyber Insurance

Marsh McLennan, one of the leading cyber insurance underwriters, established the Marsh Model, identifying 12 separate security controls that need to be addressed to meet the requirements of most cyber insurance carriers:

Marsh Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/ network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Marsh has issued a 34-page explanation[12] of these requirements, but to save you time we'll summarize them here.

[12] *marshmclennan.com/content/dam/mmc-web/insights/publications/2022/april/uscybercampaigntwelvekeycybercontrolsv31.pdf*

Multifactor authentication (MFA) for remote access and admin controls

Cyber incidents often start with compromised user credentials, and MFA is an important component of a good identity and access management (IAM) strategy. Ideally, MFA should be used to guard all systems, applications, and accounts that can be accessed by privileged users such as administrators, or remotely by any user. At a minimum, MFA should be employed on critical assets, privileged accounts, and applications with remote access requirements.

> *Note: In the previously mentioned Travelers case, the insurance provider revoked coverage because the insured organization had not instituted MFA as it asserted on its policy application.*

Email filtering and web security

Malicious links and files embedded in emails are a primary way to distribute and deploy malware in an organization, allowing an attacker to steal passwords, access critical systems, and execute ransomware attacks. Similarly, hazardous websites and web content can be sources of infiltration into a corporate network, and sites such as those used for command and control (C2) can be used to orchestrate attacks and exfiltrate data. Email and web content filtering can help limit these access points for cybercriminals and give insurers more confidence that the insured will experience fewer cyber incidents.

Secured, encrypted, and tested backups

With secure backups – preferably with storage isolated from the network – companies can help improve business resilience. Proper backups also reduce the leverage that threat actors have when using ransomware to extract payment. Organizations should test regularly to ensure data and services can be restored from backups if needed.

Privileged access management (PAM)

Privileged access management helps protect accounts, credentials, and operations by limiting a user's access to the minimum level needed to perform their jobs. The same concepts can also be applied to device communications and is especially useful for unmanaged devices or those not associated with a specific user. With a PAM tool, access policy can be defined and monitored with alerts flagging any anomalous usage. Companies should consider applying PAM by identifying the critical assets that are of highest risk for exposure, then expanding scope as needed.

Endpoint Detection and Response (EDR)

EDR is essential because of how common endpoint attacks have become, jumping 68% in 2020 alone. Using this threat-detection and response technology helps organizations quickly recover from attacks thanks to enhanced visibility into where the intrusion took place and how many endpoints were affected. Organizations should implement EDR for all endpoints and have an integrated solution that includes threat intelligence and automated response policies.

Patch management and vulnerability management

Organizations need methods to identify areas of their software and hardware that are vulnerable and likely to be targets for attackers. When patches are available to address vulnerabilities, vulnerability and patch management tools will help organize, prioritize and track remediation efforts. Without clear visibility of existing vulnerabilities and a priority-driven method of patching them, organizations will struggle to identify the most critical risk and respond in an efficient, logical manner.

Cyber incident response planning and testing

Security teams must be prepared to respond to incidents quickly, efficiently, and effectively. That requires having well-defined disaster-recovery and business-continuity plans in place before an incident. Plans should not only define the processes but also define the roles and responsibilities for the individuals tasked with carrying them out. Cyber incident response plans should be tested and adjusted regularly to ensure they align with the current threats, organizational environment, and personnel.

Cybersecurity awareness training and phishing testing

Human factors such as workload, stress, and lack of cybersecurity skills can be significant weaknesses for an organization. Employees throughout an organization – not just those with security titles – should be trained to be aware of phishing emails, suspicious activity, and other threats that can lead to a breach. Security gap analysis should be done annually at a minimum and training should be required periodically to ensure employees are up to date on the latest attack and social engineering techniques they may encounter.

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Organizations need methods to identify areas of their software and hardware that are vulnerable and likely to be targets for attackers. When patches are available to address vulnerabilities, vulnerability and patch management tools will help organize, prioritize and track remediation efforts. Without clear visibility of existing vulnerabilities and a priority-driven method of patching them, organizations will struggle to identify the most critical risk and respond in an efficient, logical manner.

Logging and monitoring/network protections

Responding to suspicious activity on the network requires strong logging and monitoring capabilities, including the knowledge, tools, and processes these actions require. You may want to define and train a team that specializes in logging and monitoring because these can be complex actions for a security operations group to take on without adequate understanding and preparation.

End-of-life systems replaced or protected

Once a vendor designates a product as end-of-life (EOL) or end-of-support (EOS), it will no longer receive patches and other security updates from its vendor. Ideally, you would retire the product from service, but this isn't always possible or practical. Compensating controls, such as removing Internet access and restricting internal network communications, may be a suitable substitute approach to reduce risk. Particularly in organizations with extensive operational technology (OT) and/or Internet of Medical Things (IoMT) systems, it is important to be fully aware of the presence of such devices where utility may extend beyond vendor support. Coordination between the OT, IoMT, and IT security teams is paramount to identify, prioritize, and protect these devices.

Vendor/digital supply chain risk management

An area of increasing challenge, the digital supply chain, needs to be managed with a robust framework. Such a framework would include controlling digital interactions with the partner based on Zero Trust expectations, risk-based multifactor authentication, an incident response playbook for vendor/digital supply chain scenarios, service agreements, security training, and the like. Digital supply chain vulnerabilities have had major effects, including the Log4j and Kaseya vulnerabilities. Consequently, this final area is one deserving of particular attention, complex though it may be.

What's missing on this checklist? Among Marsh's 12 Controls, "endpoint detection and response," "patch management and vulnerability management," and "end-of-life systems replaced or protected" all require visibility into assets and the risks they pose. Because you can't protect what you can't see, this suggests a need for a 13th control: **"Asset visibility"**. In addition, while alluded to in #9 ("Hardening"), **"Segmentation"** should ideally be called out as a 14th control because segmentation and Zero Trust segmentation are important best practices to reduce risks and prevent lateral movement. In the next section, we recommend some additional considerations for security leaders and provide an overview of how Ordr can help address these requirements.

How Ordr Can Help With Cyber Insurance

The Ordr connected device security platform offers substantial help for CISOs who seek to both provide their organization with the best possible security they can attain as well as qualify for the cybersecurity insurance they seek.

Ordr's platform addresses cybersecurity requirements that have proven to be immensely useful to security leaders in cyber insurance discussion. In one organization, the security team mentioned that it **"knocked the underwriter's socks off"** when he described how they used Ordr to identify all devices, track behaviors, and help drive policy for proactive hardening with segmentation.

Here are some ways that Ordr can help with reducing cybersecurity risks and supporting cyber insurance negotiations:

Asset inventory

Ordr provides automated discovery of every asset including IT, IoT, IoMT, OT and cyber-physical systems to ensure total visibility and accountability into your entire managed and unmanaged connected device inventory. Asset visibility is foundational to cybersecurity, and required in order to meet Marsh's guidelines. This is coupled with device classification and real-time baselining of device communication flows to keep you apprised of the status of each connected asset, its configuration, vulnerabilities, communications pattern, and unusual activity.

Monitor and identify malicious east west and external communications

As described earlier, because Ordr visibility includes device and flow context, Ordr continuously analyzes device communications and can identify devices connecting to potentially malicious sites such as C2 servers used in malware and ransomware attacks or domains in risky geographies such as Russia or North Korea. It also identifies active exploit attempts using an integrated Intrusion Detection System (IDS) and alerts security teams of devices behaving outside of normal communications patterns by using machine learning technology to identify abnormal behavior. You can then use Ordr to quarantine devices on the network with a single click or generate a policy to proactively segment and isolate high-risk devices while keeping them operational. Policy is dynamically generated by Ordr and enforced through integration with your existing security and network infrastructure such as network switches and firewalls.

PAM auditing

Privileged access management is critical to ensure that threat actors do not gain administrative privileges that allow them to move laterally to a critical part of the network. Ordr identifies devices that use supervisory protocols like RDP, Telnet and SMB, associates them with user names, correlates them with the network they logged in, and maintains an accurate access record for each and every device as well as each and every user. Ordr also provides very robust tracking of users using Active Directory (AD)/RADIUS and wireless integration, enabling security teams to monitor which user is accessing what device at what time. Ordr provides two key perspective:

User tracking – analysis of all devices accessed by a user.

Device tracking – analysis of which users were logged into a specific device, at what time, duration and more.

Identify security coverage gaps

Endpoint and mobile devices depend on EDR or Mobile Detection and Response (MDR) solutions to ensure they are secure. As described in the Marsh requirements, these are a critical security control. However, security teams may not be aware of how many of these devices actually have EDR or MDR agents deployed. Ordr fills this gap by identifying where security coverage is missing. In addition, Ordr integrates with EDR and MDR solutions to enrich device insights and provide teams with a centralized view across all managed and unmanaged devices.

Patch and vulnerability management

Ordr collects details for each device, including the operating system, firmware, installed software, and patch levels. The solution matches this with vulnerabilities from National Vulnerability Database, manufacturer and FDA databases, and integrates with other vulnerability management tools like Rapid7, Tenable, and Qualys. With these details, Ordr identifies devices with vulnerabilities, unpatched and unauthorized software, or those running outdated or unsupported operating systems that cannot be patched.

Administrators can trigger IT Service Management (ITSM) and Computerized Maintenance Management System (CMMS) tickets from the Ordr dashboard to patch these devices, or take action to either quarantine devices or apply compensating controls with a dynamically created Zero Trust policy.

Identify end-of-life systems

As devices reach the point that their manufacturers no longer provide security updates, organizations need to either eliminate such devices or take a more active role in protecting them. Healthcare and manufacturing organizations in particular find this an essential activity as high-capital equipment reaches EOL support but continues to contribute to critical operations. Ordr identifies devices running EOL operating systems and integrates with a wide range of device manufacturers and government databases to identify devices with recall or EOL status.

What's more, Ordr can create Zero Trust segmentation policies to restrict device communications to those essential for operations. With this approach, Ordr helps organizations defer the cost and complexity of upgrades while keeping EOL devices protected and operational.

Incident response

During an incident, in order to move from "detection" to "response," security teams need to know details such as what device is being compromised, where it is located, and what security or compensating controls are available to quickly address the incident. Ordr provides device context and dynamically generates policies to help security teams take quick action – block traffic, terminate sessions, and quarantine devices with enforcement on existing security and network infrastructure.

Segmentation

Segmentation is a proven strategy to minimize avenues for lateral movement and mitigate risks. Device context is essential for creating and enforcing Zero Trust policies such as NAC and segmentation. Ordr automatically identifies and classifies each device with a high level of accuracy and maps traffic flows to establish baseline communication patterns and behavior. This context enables Ordr to automatically generate Zero Trust segmentation policies that reduce the attack surface and ensure each device is constrained to essential communications and nothing more, thus reducing exposure.

Logging and monitoring

Ordr continuously analyzes device communications to detect and alert teams to malicious activity. Alerts and details of devices and their communications can be sent to log management and security information and event management (SIEM) tools to provide security teams with the insights required for incident response and forensics efforts. Ordr generates insights to help security teams respond to attacks, identify all impacted devices to understand the scope of an incident, and update policies and playbooks to prevent future security events. Ordr also simplifies compliance with a wide range of regulatory standards and allows a team to concentrate on specific compliance requirements, device types, or attributes.

Vendor/digital supply chain risk management

Ordr's real-time asset inventory makes it easy to maintain a view of all deployed devices. Combined with Ordr Software Inventor Collector, Ordr also delivers detailed application insights for every device similar to a real-time SBOM (software bill of material) regardless of whether it is managed or unmanaged, online or offline, remote or on-prem. With these insights, security teams can identify impacted devices during a zero-day vulnerability disclosure.

All capabilities and benefits of Ordr are delivered seamlessly and without device agents or active scanning. Ordr's method of passively collecting a mirror of network data for analysis will not impact your mission-critical connected devices and with over 80 integrations across the security, network, and IT infrastructure, Ordr provides granular device insights to enrich existing tools, accelerate security efforts, and improve protection for all your connected devices.

And Finally: Lowering Cyber Risks Means Lower Costs

We encourage readers to watch the Ordr of Business Webinar[13] on cyber insurance for more insights on lowering cyber risks.

Improving your security posture and lowering cyber risks will continue to pay dividends for security leaders. While cyber insurance coverage may be getting harder to procure (or more expensive), security leaders who have invested in critical cybersecurity technologies and built the right processes within their organizations have enjoyed lower premiums because of confidence in their cybersecurity programs, and their lower risk profile.

The Ordr connected device security platform, with the visibility, automation, and policy-creation/enforcement mechanisms it includes, can speed you along the path to enhanced security and control. To discuss your situation and how Ordr can assist you in achieving your objectives, please contact us.

[13] *https://resources.ordr.net/resource-center/cyber_insurance_webinar?lx=B0MdQI*

CONTACT US

ordr