Cyber Insurance Assessment Readiness Checklist

The booming cyber insurance market is a reaction to the explosion of cyberattacks and data breaches in the last few years. In 2021, attacks increased 50%, much more than businesses or insurers expected or budgeted for.

Given that most cyber incidents involve compromised credentials, it's no wonder insurance companies are tightening requirements related to Privileged Access Management (PAM). Specifically, insurers are taking a close look at how well businesses follow PAM practices such as granular access control, Multi-Factor Authentication, and the principle of least privilege to protect privileged accounts and systems.

While each insurer will have its own methodology to assess risk, the questions below are ones they're likely to ask you. The questions are grouped according to the five key functions of the National Institute of Standards and Technology's (NIST) cybersecurity framework (Identify, Protect, Detect, Respond, and Recover) and focus on reducing risk for the most common and vulnerable attack vector — privilege.

The more completely you can answer these questions on the next few pages, the more likely you are to obtain a cyber insurance policy at a rate that reflects your risk.

Let's get started.

Insurers may ask	Why they want to know	How you can prepare
Identifying your risks		
How do you identify threats, vulnerabilities and risks?	Insurers want to know that you understand your risks and have established risk management processes.	Understand your company's risk profile by conducting a cybersecurity risk assessment. Identifying your vulnerabilities will also help you gauge your company's cyber risk tolerance.
How do you educate employees and vendors about cybersecurity?	Humans are a high security risk in most organizations. Insurers want to see that you conduct recurring cybersecurity training that extends beyond simple online tests or signoffs on security policies.	Make cybersecurity awareness training a fundamental part of your corporate culture — include it anytime you conduct company-wide or departmental training. Updating employees on the latest phishing tactics and social engineering schemes can go a long way toward protecting your organization.
Do you maintain inventories of hardware, software, and privileged accounts?	You should have a list of all devices, applications, and privileged accounts that could be a possible entry point for malicious attacks.	Compile an inventory of all devices, software, and privileged accounts used across your company, including those used by remote workers. This will help you identify all threat vectors and determine the value and scope of the assets you want to insure. Discovery tools for Active Directory accounts and passwords, service accounts, and local accounts and applications help you identify shared accounts, accounts that have expired, and accounts that are no longer needed.
Do you use Multi-Factor Authentication to validate who is accessing your systems?	They want to know that you're authenticating users with more than just a password.	Multi-Factor Authentication (MFA) adds an additional layer of security for access control. MFA shows insurers that you're minimizing exposure to credential-based cyberattacks, so be sure to use it everywhere — at login and at privilege elevation.
Protecting your assets		
Do you automate password management?	Insurers want to see that you're not relying on manual spreadsheets for password management. Adopting privileged password management software allows you to securely create, share, and automatically change enterprise passwords and manage privileged security.	Implement a privileged password management tool to track credentials and generate and rotate complex passwords for all your accounts so people won't have to type or remember them. Automation ensures policies are applied consistently and avoids human error.
Have you implemented Privileged Access Management (PAM)?	By delineating the boundaries of of access to your systems, you show insurers that you're protecting your privileged accounts from malicious hackers who might conceal their activities in the guise of a legitimate administrative user.	Implement a comprehensive PAM solution to help you control access to systems and sensitive data and comply with regulations. Look for software that automates the identification and analysis of risk to your privileged accounts, along with vaulting, continuous monitoring, and session recording.

Insurers may ask	Why they want to know	How you can prepare
Protecting your assets (continued)		
What kind of malware defense have you deployed?	Insurers will expect you to have multiple layers of malware defense to protect against viruses and rouge programs deployed bad actors.	Prevention is the best defense. Demonstrate to insurers that you're taking every feasible measure to protect your company from malware attacks by implementing defense-in-depth. This includes implementing and enforcing least privilege access, restricting or removing local admin rights, and layering in threat intelligence and endpoint protection solutions for both workstations and servers.
If an attack renders your privileged accounts and passwords inaccessible, do you have a backup plan?	When disaster strikes, it's critical to recover quickly. If your cloud or data center environment has been compromised, you have a single point of failure that blocks your ability to recover from a disaster.	Make sure secrets (passwords and other credentials) aren't tied to a single location and can be moved to a safe space if necessary. Any password management or PAM solution should have infrastructure redundancy for break-glass access.
Detecting risk and breaches		
Do you have endpoint security in place?	The increase in remote work means that more endpoints, such as laptops and tablets, as well as cloud servers, are prime targets for attacks. If you have an endpoint security tool it will be easier for you to identify and respond to cybersecurity events originating at your endpoints.	Choose an endpoint security solution that can provide comprehensive monitoring, alerting, and reporting capabilities for privileged behavior on workstations and servers. This will allow your IT security team to identify unexpected behavior and conduct forensic analysis if a breach occurs.
What type of credential monitoring have you implemented to track privileged account usage?	There's a good reason cyber insurers expect you to keep an eye on your employees' credential usage: 60% RSA conference respondents identified employees as the greatest risk to their organization's cybersecurity.	Empower remote employees and vendors to follow security best practices for privileged account usage, no matter where they work. Leverage a PAM solution that can monitor remote sessions, extend remote monitoring to cloud sessions, and uses Privileged Behavior Analytics to detect anomalies and stop attacks.
Responding to cyber attacks		
Do you have incident response plans, and how often are they tested and updated?	Insurers expect you to have an incident response plan because it can reduce the risk of a cyber breach becoming a catastrophe. It helps enable your IT operations, security, and incident response teams to form a united front against an attack, coordinate a rapid response, and maintain your business continuity.	Use a customizable template to create an incident response plan that matches your risk profile, regulatory requirements, and organizational structure. Include a checklist of roles and responsibilities and actionable steps to measure the extent of a cybersecurity incident and contain it before it damages critical systems. Conduct incident simulations to help you identify areas for improvement and demonstrate to insurers that your readiness is more than theoretical.

Insurers may ask	Why they want to know	How you can prepare
Responding to cyber attacks (continued)		
What type of incident response tools do you have in place to detect privileged account attacks?	Insurers know that firewalls and antivirus tools aren't sufficient to detect and shut down sophisticated cyberattacks. They want to see that you're using PAM tools to detect breaches and coordinate an effective response.	Reduce the potential effort and cost of incident response by layering privileged access security across your workstations and servers. Choose tools that validate identity, enforce MFA for access to privileged accounts, manage passwords, and detect unusual behavior.
Recovery after an attack		
If a cyber incident occurs, how would you fix the security gaps that made your organization vulnerable?	Your recovery plan is vital for getting your business up and running again, and for preventing future security incidents. Insurers want to see that you have plans in place to quickly return your operations to normal and stem your losses.	Don't make the mistake of being overoptimistic about your recovery abilities. Although 71% of companies are confident they can quickly recover from a cyberattack, real experiences tell a different story. It takes an average of 280 days to identify and contain a data breach. Demonstrate to insurers you're realistic, willing to learn from cyber mistakes, and implement ongoing improvements.

Next Steps and Additional Resources

Get more detailed recommendations to evaluate and reduce your privileged access risk with Delinea's PAM Checklist.

FREE TOOLS Discover your security vulnerabilities before insurance companies ask you.

Windows Privileged Account Discovery

Least Privilege Discovery

Service Account Discovery

Browser-Stored Password Discovery

Delinea

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide, including over half of the Fortune 100. **delinea.com**