hackerone

Build a Resilient Cyber Risk Strategy with Hacker-Powered Security and Cybersecurity Ratings

Table of Contents

Cyber Risk is Difficult to Get Right

A risk-based cybersecurity strategy is essential to protect today's organizations effectively. Accurate risk profiling informs better business decisions, budget allocation, and security outcomes. However, cyber risk is difficult to measure and even harder to track over time.

When organizations identify their specific cyber risks, discover the most crucial vulnerabilities, and map these findings to quantifiable measurements of overall cybersecurity performance, they can develop effective security strategies to mitigate risk and protect against attack.

Common Sources of Cyber Risk

Internal

- Vulnerabilities in digital assets
- Infrequent patching cadence
- Unprotected coding practices
- Asset misconfiguration
- Privilege or access misuse

External

- Malicious hacking, including misuse of legitimate business logic
- Unknown and zero-day threats
- Third-party risk from supplier partners and mergers and acquisitions

How to Measure and Mitigate Cyber Risk

Most organizations face at least some risk from all of the above sources. However, historically, calculating the risk of different threats has proven difficult and complex.

Several methods attempt to solve the problem by combining threat intelligence with mathematical models, but these approaches all require a significant investment of time and resources. Many organizations try to track cyber risk against common frameworks. This approach works to some degree but relies on manual assessments that are time-consuming and quickly outdated.

Today, cybersecurity rating platforms simplify both measurement and mitigation. Formerly the exclusive domain of large financial and telecom providers, risk-based security programs are now within reach for any organization.

Mitigating Cyber Risk

Once the risk is measured, the process for remediation is straightforward:

Step 1: Identify sources of cyber risk

Step 2: Drill down to the source of each threat

Step 2: Rank threats according to the risk they pose

Step 3: Take appropriate mitigation steps

For example, mitigating the risk associated with a vulnerability usually involves patching the vulnerability, or in the case of internally-developed applications, making code improvements.

However, organizations still face a challenge. Identifying all possible security vulnerabilities isn't easy in a landscape where threats evolve faster than protective controls.

Security teams use scanning tools and internal testing to uncover common vulnerabilities, but this approach doesn't find more complex issues like chained exploits and business logic abuse attacks. In the past, organizations turned to security testing providers to find these complex issues. However, scheduling delays and limited talent pools have caused this approach to become less effective in protecting digital assets against today's threats.

Hacker-Powered Security: What it is and How it Works

Hacker-powered security enlists the global ethical hacking community to discover crucial security vulnerabilities and reduce cyber risk. Organizations can improve their security profile by working with hackers to identify high-risk, exploitable issues missed by automated scanners and internal testing.

Hacker-powered security provides organizations with:

- Access to people with skills and expertise that aren't otherwise readily available
- Access to a large and diverse community of specialized hackers
- Capacity to manage sudden surges in testing requirements without hiring full-time staff

These capabilities make hacker-powered security ideal to identify some of the most common sources of cyber risk described above. In particular, hackers regularly uncover issues such as:

- Asset misconfiguration
- Vulnerabilities not discovered by scanners
- Unprotected coding practices
- Business logic abuse attacks

YoY Growth Of The Top Ten Vulnerabilities	
1. Cross site scripting	+23%
2. Information disclosure	+65%
3. Improper access control	+53%
4. Improper authentication	+44%
5. Privilege escalation	+54%
6. Insecure direct object reference	+49%
7. Cross site request forgery	+7%
8. Server side request forgery	+18%
9. SQL injection	+48%
10. Code injection	+19%

Ethical Hacking

The HackerOne community grew by 63% in the last year. Top hackers reported vulnerabilities across an average of 20 threat categories, and HackerOne customers saw a significant rise in verified reported vulnerabilities.

But who are these hackers?

The 2021 Hacker Report found that 82% of hackers are part-time, and 35% have full-time jobs, often as security researchers and penetration testers. Many community members have a technical background—37% have postgraduate computer science experience, and 20% hold other doctoral qualifications.

How Hacker-Powered Security Works

At the most basic level, hacker-powered security falls into two categories:

Vulnerability Disclosure Programs (VDPs) set clear guidelines for hackers to search for and submit vulnerabilities in defined assets and systems. VDPs harness the drive and creativity of the hacking community to provide a continuous source of new vulnerabilities.

Bug bounty programs take this concept to the next level by incentivizing hackers to search for vulnerabilities in defined applications, assets, and systems. Organizations publish the guidelines of their program, including a monetary reward for attracting the attention and expertise of top hackers.

Organizations can also enlist the help of external hackers through time-bound engagements:

- Assessments in the form of penetration tests
- Challenges where organizations invite hackers to focus on a specific event for a concentrated period
- Controlled engagements with highly-vetted, specialized hackers

Supporting Vulnerability Management

Vulnerability Management programs use a simple five-step cycle:

1. **Discover** the external attack surface and find externally exploitable vulnerabilities
2. **Assess** discovered vulnerabilities and how much risk they pose to the organization
3. **Remediate** each vulnerability
4. **Verify** that remediation steps have been successful
5. **Refine** the program by tracking KPIs and benchmarking against similar organizations

Vulnerability Management relies heavily on automated vulnerability scanners. A typical scan uncovers hundreds of known vulnerabilities but provides little context for the severity of risk they represent even though they are listed in the CVE database. As a CVE Assignment Authority (CNA), HackerOne can work with customers to disclose vulnerabilities and publish them to MITRE with an assigned CVE ID for consistent reference.

Vulnerabilities reported by hackers via an established program provide organizations with a report of high-risk, exploitable vulnerabilities. These reports highlight the risks that matter most and aren't limited to bulk vulnerabilities. Hacker-powered security from HackerOne provides organization-specific risk ranking, remediation guidance, and retesting to ensure the successful completion of remediation steps. HackerOne programs also provide easy KPI tracking and benchmarking to help organizations make their Vulnerability Management programs more effective.

Manage Cyber Risk with Hacker-Powered Security

As noted earlier, a significant challenge of cyber risk management is determining how much risk is posed by specific threats. For example, it's essential to know if a software asset has a vulnerability, but that information alone doesn't tell the whole story. An organization must measure the risk posed by each vulnerability to know which to resolve first.

Earlier, we looked at a four-step process for cyber risk reduction. Figure 2 shows how hacker-powered security supports each step.

Step	Objective	Hacker-powered security provides:
1	Identify sources of cyber risk	Ongoing testing coverage of the entire internet-connected environment
2	Drill each source down to the individual threats involved	Continuous vulnerability reports from a diverse pool of skilled hackers
3	Rank threats according to the posed risk	Validation and risk scoring before passing vulnerabilities to the organization
4	Take appropriate mitigation steps	Complete documentation, including guidance on how to recreate and remediate the vulnerability

With a constant supply of risk-ranked reports, organizations can systematically tackle the highest severity vulnerabilities first. This approach has a more significant impact on overall cyber risk levels than resolving vulnerabilities in the order of reporting.

Cybersecurity Ratings

Cybersecurity Ratings

Cybersecurity ratings are like a credit check for security readiness. Rating providers use powerful engines to review an organization's attack surface, evaluate its ability to protect assets and data, and assign an appropriate score. This score updates continuously as the organization's attack surface and security controls evolve, providing an accurate, real-time portrait of its security resilience.

How Cybersecurity Ratings Work

Similar to those used by credit agencies and insurers, cyber rating providers use intelligent platforms to produce category and cumulative ratings for each organization. These ratings consider an organization's externally visible attack surface identified security issues, and analytics generated by the provider's threat intelligence researchers, data scientists, and software engineers.

Rating platforms use a three-stage process to calculate cybersecurity ratings:

1. **Attribution:** A customer supplies their top-level domain, and the platform scans the IPv4 address space to identify all domains, subdomains, IP addresses, WHOIS records, redirects, and SSL certificates associated with it. This process discovers the entire external attack surface, including any third parties digitally connected to the organization.
2. **Signal Collection:** For every asset identified during attribution, the platform completes a thorough scan to identify signals like certificates, IP addresses, headers, etc., and adds them all to the platform's data lake.
3. **Scoring:** Once the platform can see all of its assets and signals, it grades them using a rating engine. Every piece of data is assessed against compliance and best practice frameworks like PCI-DSS, NIST CSF, ISO 27001, and many more to determine an overall score.

While this three-step process appears simple, the behind-the-scenes processes are based on complex cyber and mathematical analysis. For a detailed overview, read this eBook.

Real-World Uses of Cybersecurity Ratings

While there are many uses for cybersecurity ratings, three use cases stand out:

Enterprise monitoring

Maintaining an effective cybersecurity program is more challenging than ever. Overlooking a single weakness can mean a program that was secure yesterday could be penetrable tomorrow. As bad actors exploit new vulnerabilities and breach organizations with household names using simple, low-skill attacks, this cycle repeats.

Reliance on static indicators and measurements created challenges. While these may provide accurate information at a point in time, they quickly go stale, forcing organizations to rely on outdated information or allocate significant resources to assess their cybersecurity programs continually. Cyber rating platforms avoid these issues by providing instant, continuously updated ratings based on objective analysis. These ratings allow security leaders to make fast, accurate decisions and react quickly to changes in the threat landscape.

Vendor risk management

A recent Ponemon Institute study found that 44% of organizations had suffered a third-party-related breach in the previous 12 months. Most organizations are aware of these risks but don't have the visibility and authority over them.

Traditional approaches to measuring third-party risk are time-consuming, slow, inaccurate, and outdated upon completion. In many cases, assessments either don't happen or are less thorough because organizations don't have the time or resources to complete them for every vendor and partner.

Cybersecurity rating platforms can help. An organization can point the platform at the relevant top-level domain and assess the third party. Within minutes, the risk associated with different vendors can be identified and benchmarked. Even better, ratings update over time, allowing organizations to keep track of third-party risk and intervene if a score falls below an established threshold.

Compliance

Compliance is of significant concern in the cybersecurity world. Many frameworks are descriptive rather than prescriptive, and successful completion of a compliance requirement may be subjective and in auditors' control. When an organization is cited for compliance issues, there is no guarantee that a compliant system or process will be approved.

A comprehensive cybersecurity rating scorecard provides objective, independent validation to auditors and other third parties that an organization is committed to a strong cybersecurity profile. Specifically, the scorecard can demonstrate a consistent and practical approach to identifying and resolving security weaknesses.

This rating can be the difference between compliance and non-compliance, particularly if the assessment is completed after a security breach.

How HackerOne and SecurityScorecard Support Effective Risk Assessment

HackerOne has partnered with SecurityScorecard to help organizations get a comprehensive picture of their cybersecurity risk profile. The integration allows SecurityScorecard customers to see hacker-powered security signals and data within their scorecard, including the latest hacker activity. For the first time, insights, KPIs, and benchmarks from hacker-powered security programs integrate directly into cybersecurity scorecards, determining the effectiveness of an organization's security program. Accurate vulnerability intelligence can be used as a leading indicator to identify and resolve high-risk security issues before malicious actors can exploit them.

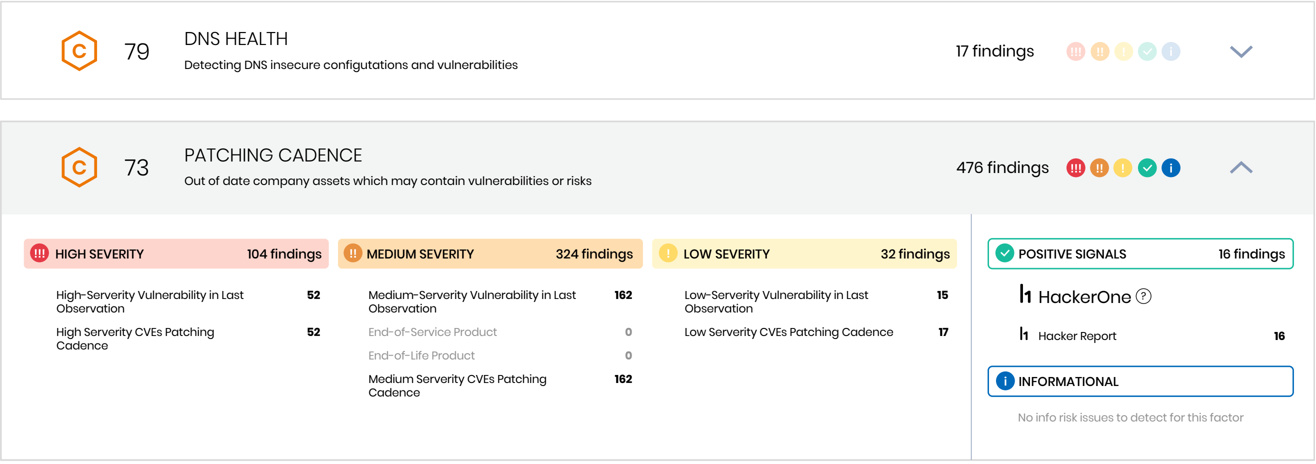
Partners and other third parties can also use hacker-powered signals to augment their existing vulnerability management efforts and extend the reach of their risk reduction strategies. Similarly, organizations can use the new insights such as vulnerabilities resolved, mean time to remediation, and more to demonstrate the success of their vulnerability management programs to prospective partners, customers, and compliance assessors.

A Comprehensive View of Cybersecurity

HackerOne’s community-led approach provides the broad range of expertise needed to uncover new or complex vulnerabilities, while SecurityScorecard’s technology-led approach provides rapid, ongoing detection of known vulnerabilities. The two solutions provide a continuous view of the entire cyber risk profile.

The combination of hacker-powered security and cybersecurity ratings gives organizations an accurate view of their cybersecurity position.

By proactively strengthening their vulnerability management with hacker-powered security, they gain a quantifiable improvement in their risk profile. Security teams can use SecurityScorecard data to guide the scope of hacker-powered security programs while using the data from those programs to enhance cybersecurity ratings and risk profiling accuracy as shown in Figure 2 below.



C 79 DNS HEALTH

Detecting DNS insecure configutations and vulnerabilities

17 findings

C 73 PATCHING CADENCE

Out of date company assets which may contain vulnerabilities or risks

476 findings

HIGH SEVERITY	104 findings
High-Serverity Vulnerability in Last Observation	52
High Serverity CVEs Patching Cadence	52

MEDIUM SEVERITY	324 findings
Medium-Serverity Vulnerability in Last Observation	162
End-of-Service Product	0
End-of-Life Product	0
Medium Serverity CVEs Patching Cadence	162

LOW SEVERITY	32 findings
Low-Serverity Vulnerability in Last Observation	15
Low Serverity CVEs Patching Cadence	17

POSITIVE SIGNALS	16 findings
HackerOne ?	
Hacker Report	16

INFORMATIONAL

No info risk issues to detect for this factor

Augmenting the Vulnerability Management Cycle

This v and SecurityScorecard integration delivers comprehensive identification and resolution of high-risk vulnerabilities throughout the Software Development Life Cycle (SDLC). Continual testing of the cyber risk associated with third parties and internet-facing infrastructure assures that safer applications are built and deployed.

Together, hacker-powered security and cybersecurity ratings enable organizations to ensure risk reduction at every stage of the vulnerability management lifecycle.

Controlling Risk with HackerOne and SecurityScorecard

Guiding internal risk assessment and improving cybersecurity profile

SecurityScorecard provides an accurate, real-time assessment of an organization's risk profile. By highlighting risk areas, the platform helps organizations set the scope of hacker-powered security programs to identify and resolve weaknesses in those areas. Through this process, an organization can reduce cyber risk in those areas and improve its cybersecurity posture.

By incorporating hacker-powered results and indicators, HackerOne helps enrich the accuracy of SecurityScorecard's ratings, giving organizations a complete picture of their cybersecurity risk profile. Similarly, SecurityScorecard's continuous monitoring helps track the success of hacker-powered security programs by demonstrating the impact those programs have on an organization's cumulative and category ratings.

Tracking and reducing third-party risk

Third parties represent a considerable risk to an organization. Using SecurityScorecard, organizations can fully picture how effectively suppliers and partners harden their attack surface over time, aiding in selecting suppliers and partners and negotiating with existing third parties if they pose a significant risk.

Using hacker-powered program data and insights, organizations can get a comprehensive view of third parties' risk and security profiles, allowing for fast, accurate decision-making, reducing the cybersecurity risk associated with third parties.

Hacker-powered security program data provides an enhanced scorecard for organizations aiming to win business and forge new partnerships. This scorecard demonstrates to third parties that the organization takes security seriously and will not pose a security risk to other organizations, a potential factor in winning new business.

How leading indicators can reduce risk

To learn more about how HackerOne and SecurityScorecard help organizations build a resilient cyber risk strategy, watch our recorded workshop with Alex Rice, CTO at HackerOne, and Mike Wilkes, CISO at SecurityScorecard. During the workshop, they discuss the many advantages of proactive and continuous risk assessment.

About HackerOne and SecurityScorecard

HackerOne

HackerOne partners with the largest and most diverse hacker community in the world to surface our customers' most relevant security issues before criminals can exploit them. Our continuous testing platform helps organizations mitigate security risks by allowing systematic testing at every level of the SDLC. Hacker-powered security helps security teams increase visibility, manage costs, and address evolving threats with consolidated, scalable security solutions.

HackerOne was started by hackers and security leaders driven by a passion for making the internet safer, and our platform is now the industry standard for hacker-powered security. HackerOne is headquartered in San Francisco with offices in London, New York City, Singapore, and the Netherlands.

Find Out More

SecurityScorecard

SecurityScorecard is the global leader in cybersecurity ratings, with over two million companies continuously rated. Over 1,000 organizations use SecurityScorecard's patented rating technology for self-monitoring, third-party risk management, board reporting, and cyber insurance underwriting. The platform enables organizations to become more resilient by allowing them to easily find sources of cyber risk and fix security issues across their external digital footprint in real-time and map issues to 15 different compliance frameworks.

Find Out More