5 Steps to Avoid a Cyber Incident and Save Your Company Millions

SecurityScorecard

According to a recent Gartner report[1], by 2025, a lack of talent or human failure will be responsible for over half of significant cyber incidents. And with the average cost of a data breach[2] now at $4.35 million, it's time for organizations to take proactive measures to protect themselves against cyber threats. This ebook was written with experts from SecurityScorecard's Digital Forensics and Incident Response team, who have decades of experience working with companies to respond to cyber incidents. Here, these experts provide practical guidance for protecting your organization against cyber threats and mitigating their associated risks for CEOs and CISOs.

The average cost of a data breach is

$4.35 million[2]

Most security professionals cite cybersecurity as a primary concern but don't necessarily have the tools to prioritize it and effectively protect their companies. Implementing **THESE FIVE STEPS** will help to avoid significant disruption of service and reputational damage, while saving your organization millions of dollars:

1. **Set a cybersecurity budget for your company**
2. **Properly assess your incident response team's capabilities**
3. **Clearly define how you respond to a cyber incident**
4. **Know the specifics of your cyber insurance policy**
5. **Proactively strengthen your cybersecurity posture**

CHECK OUT THE CHEAT SHEET

1. "Predicts 2023: Cybersecurity Industry Focuses on the Human Deal", Gartner, 2023
2. "Cost of a data breach 2022: A million-dollar race to detect and respond," IBM, 2022

STEP 1

Set a cybersecurity budget for your company

Setting a cybersecurity/information security budget is a critical starting place in order to operate safely in the digital world. It is essential to recognize that there is no such thing as 100% protection from cyberattacks. Threat actors are constantly evolving their tactics, and new vulnerabilities can be discovered at any time. Thus, the goal of cybersecurity is not to achieve perfect protection, but to mitigate risk and minimize the impact of a successful attack.

A good starting point is to allocate a percentage of your overall information technology budget to cybersecurity, typically ranging from 5-15%. This budget should be used to invest in a range of measures, including network security, endpoint protection, access controls, cyber insurance, and security awareness training for employees.

Cyber Defense Tools

Conduct an inventory of the cyber defense tools you have in place to protect your company's networks, devices, and data from cyberattacks. Examples of cyber defense tools include: antivirus software, firewalls, intrusion detection systems, and encryption software.

When deciding on tools, the traditional approach of siloed and "best of breed" can no longer scale to address an ever-expanding attack surface, leaving infosec teams creating manual processes and integrations to increase efficiency. Tackling one problem at a time isn't a sustainable option, which is why organizations must adopt a more cohesive solution with a multi-prong approach that reduces their attack surface and tests cyber defenses.

While not necessarily a security tool, automated data backups (also called live backups) have become a must-have resource in recovering from a ransomware attack. With new adversarial efforts such as "double extortion," paying a ransom doesn't always guarantee getting your data back. With automated data backups, you can restore your data to a previous point in time before the attack occurred, allowing you to recover without paying the ransom.

Are you using these cyber defense tools to secure your environment?

- Firewall and Intrusion Detection System, Web Filtering, Sandbox, DNS security
- Endpoint Protection
- Identity & Access Management
- Email Protection Services
- Extended Detection & Response (XDR) and Endpoint Detection & Response (EDR)
- Web Application Scanner
- Security Information and Event Management (SIEM) or Networking Monitoring & Log Management
- Security Orchestration Automation Response (SOAR)
- Third Party Cyber Risk Management with a Ratings Service
- Attack Surface Management (ASM)

INCIDENT RESPONSE & DIGITAL FORENSICS TEAMS

An incident response team manages and implements the cybersecurity strategy for your company to identify and mitigate risks and enhance its overall cybersecurity posture. This team can include in-house or outsourced experts. Typically, investing in an in-house team can be cost-prohibitive, which is why companies can save money by leveraging outside cybersecurity and incident response experts to conduct investigations and other forensic services.

PROACTIVE MEASURES AND SERVICES

There are proactive measures and services your company can leverage to reduce the likelihood of a cybersecurity breach and also limit the damage if one does occur. These can include: tabletop exercises that simulate a cyber incident; red team & penetration test exercises that actively probe and test your environment; threat intelligence for gathering information on threats and vulnerabilities; and regular employee security training. For a deeper dive into tips for staying proactive, see Step #5.

INVESTING IN CYBER INSURANCE

Cyber insurance provides the financial resources to ensure that your company can cover the cost of legal fees, data recovery, and other breach-related expenses. In addition to the financial element, cyber insurance can also connect policyholders with the service providers who will guide them through the incident and recovery process.

Questions to ask when evaluating your cyber insurance policy:

- What's covered? What's not covered? What is the deductible?
- How does external cyber risk exposure inform underwriting decisions?
- Do I get to choose my own cyber responders?
- What are the requirements to obtain coverage?
- Which cyber ratings services do you base your assessment on?
- Which security improvements can I make to obtain preferential pricing and coverage terms?

Cybersecurity is not just a one-time exercise, but an ongoing investment.
It's essential to regularly assess and update your cybersecurity measures to stay ahead of potential risks.

STEP 2

Properly assess your incident response team's capabilities

The first priority in any incident response program is preparation. This means assessing where your team stands in terms of its response capability. Identifying any gaps or weaknesses allows you to take proactive measures to improve response readiness and minimize the impact of potential incidents. The assessment should include key areas, such as: incident detection and identification; containment and eradication; recovery and restoration; and post-incident analysis and reporting.

A well-tested team is an efficient team and can **save an average of $2.66 million** in breach costs.[1]

While most digital forensic firms don't provide references, it is important to ask about their standard operating procedures (SOP) during an incident, such as:

+ What is their Service Level Agreement (SLA) in terms of time to meet with you should you have an incident and need their help?
+ Will they assist with your Endpoint Detection & Response (EDR) management? If not, will they deploy an EDR? Which EDRs do they normally work with?
+ How do they investigate third party breaches?
+ When do they take forensic images of a machine?

Critical questions to ask when evaluating your incident response team:

Do you have experience responding to a wide range of cyber incidents, such as ransomware attacks, data breaches, and phishing attempts? What about one through a third party?

Do you have experience conducting incident response exercises, such as tabletop exercises or red team assessments?

Are you able to evaluate and understand your SIEM data?

Do you have experience working with external partners, such as law enforcement or cyber insurers?

Do you have the ability to take legally admissible forensic images and conduct complex digital forensic investigations of potentially compromised devices and/or firewall logs?

Do you have experience working with media, insurance, legal, and other partners? Are these partners signed up and available should a breach occur?

Conducting due diligence in evaluating your incident response team is critical and can make a difference between saving your company or losing it in a significant cyber incident.

1. "Cost of a data breach 2022: A million-dollar race to detect and respond," IBM, 2022

STEP 3

Clearly define how you respond to a cyber incident

A cyber incident response plan (IRP) is an important asset in the case of a serious cyber incident. Most breach responses don't typically fail due to technical reasons or knowledge gaps, but due to undefined or untested IRPs. Though frequently required by an insurance company or regulatory agency, IRPs are oftentimes put in place to check a box for compliance reasons and neither built correctly nor practiced regularly. Cross-team collaboration and knowledgeable expertise are key in building an IRP. By preparing for a cyber incident, an organization is better positioned to successfully respond to a breach and strengthen its cybersecurity posture.

To ensure a well-coordinated incident response, it is essential to establish clear communication channels among all members of the incident response team and key stakeholders. A well-designed communication plan should specify who needs to be notified during an incident, the timing of notifications, and the methods of maintaining communication across departments. For additional insights, the National Institute of Standards and Technology (NIST) has a useful cybersecurity framework to help organizations build an effective incident response plan.

Reasons why cyber incident responses are unsuccessful may include:

- Lack of a clear incident response plan
- Lack of communication with key stakeholders
- Failure to follow the incident response plan
- Inadequate employee training

How your company responds to a cyber incident depends on the specific circumstances surrounding it. However, here are some general steps to consider:

CONTAIN
Isolate the affected systems to prevent the incident from spreading.

INVESTIGATE
Determine the scope of the incident and identify its cause.

RESPOND
Restore systems, recover data, and implement additional security measures.

REPORT
Disclose the incident to the appropriate authorities, such as law enforcement, regulatory agencies, etc.

Between 2020-2022, cyber insurance premiums increased

185%[1]

STEP 4

Know the specifics of your cyber insurance policy

In today's business climate, cyber insurance is an important tool for cybersecurity professionals to consider in offsetting the damage from a cyber attack. Just a couple of years ago, if you had a ransomware attack or breach, you were confident that your cyber insurance would cover the cost of paying the ransom to decrypt your environment. However, cyber insurance premiums have increased dramatically over the last two years, resulting in more strict underwriting requirements and coverage constraints. Although premiums appear to be flattening in 2023, strict underwriting and coverage constraints still remain. With that in mind, it's important to know which questions to ask when looking for cyber insurance.

Some key questions to ask about your cyber insurance policy:

What is the deductible and maximum coverage amount?

How is the premium calculated? How can you reduce its cost?

Does it cover digital forensics and incident response?

Does the cyber insurer choose the incident response companies or do you?

What kind of incidents are covered?

Are clauses included that trigger additional sub-limits or coverage exclusions?

Does it cover lost sales or downtime due to a ransomware attack? Are extortion payments covered?

Does it handle reinstatements of coverage in the event of a claim?

While cyber insurance premiums are important to consider, the type of coverage that is provided is equally important. Ransomware, data exfiltration, business email compromise, employee error, phishing attack, insider threat, and unauthorized access are all potential types of cyber-attacks to keep in mind when looking at different plans. In many cases, it's advisable to have an attorney who specializes in cyber insurance review the policy.

1. "A Hard Reset 2.0," Howden, 2022

STEP 5

Proactively strengthen your cybersecurity posture

It's crucial that organizations take proactive measures to prepare for and effectively respond to cyber incidents. The following actionable steps will test your security controls, strengthen your cybersecurity posture, and mature your incident response plan:

PENETRATION TESTS

Conduct regular penetration tests to identify any vulnerabilities in your network and systems. Penetration tests are typically carried out by trained professionals who simulate real-world attack scenarios, and provide recommendations to address security gaps and weaknesses.

VULNERABILITY MANAGEMENT

Vulnerability management helps organizations identify and address vulnerabilities before they can be exploited by attackers. This includes: regularly scanning for and continuously monitoring vulnerabilities; prioritizing them based on severity; and applying remediation measures to mitigate risk. This is an ongoing process that helps to ensure systems and networks are secure and up-to-date.

TABLETOP EXERCISES

Tabletop exercises are customized, real-life scenarios that help organizations practice their cyber incident response plans by uncovering gaps and ensuring they're ready to respond effectively and efficiently if a real incident occurs.

OBJECTIVES OF TABLETOP EXERCISES INCLUDE:

- Evaluating current cybersecurity protocols and procedures
- Identifying gaps within current processes
- Understanding roles and responsibilities of each employee involved in incident handling
- Testing internal and external communication and escalation processes with stakeholders
- Educating technical responders and senior leaders on the current cyber threat landscape

RED TEAM

Red Teams use intelligence-led threat scenarios to perform a simulated real-life cyber attack. Red Team experts use techniques and methods of known malicious groups to identify and rate the resilience of your organization, while also uncovering compromising vulnerabilities found in systems, networks, applications, physical security, or people.

THREAT HUNTING

Threat hunting is the art of proactively detecting and isolating advanced threats that evade traditional detection technology using tools such as: security information and event management (SIEM), endpoint detection and response (EDR); and more. Threat hunting helps your organization reduce its cyber risk exposure by determining the who, what, why, when, where, and how behind cyber threats.

THREAT INTELLIGENCE

Threat intelligence is the collection and analysis of information about potential or actual cyber threats to an organization's attack surface that are not typically detected by internal security controls, such as: leaked username/password credentials; leaked personal identifiable information (PII); imposter domains; social media chatter; and more. The goal of threat intelligence is to provide actionable insights to help prevent, detect, and respond to cyber attacks more effectively.

SECURITY ASSESSMENTS

Security assessments evaluate the security posture of an organization's information systems. They involve identifying vulnerabilities, weaknesses, and potential threats to assets, such as hardware, software, and data. These assessments also help to identify areas for improvement in security infrastructure and develop strategies for mitigating risk.

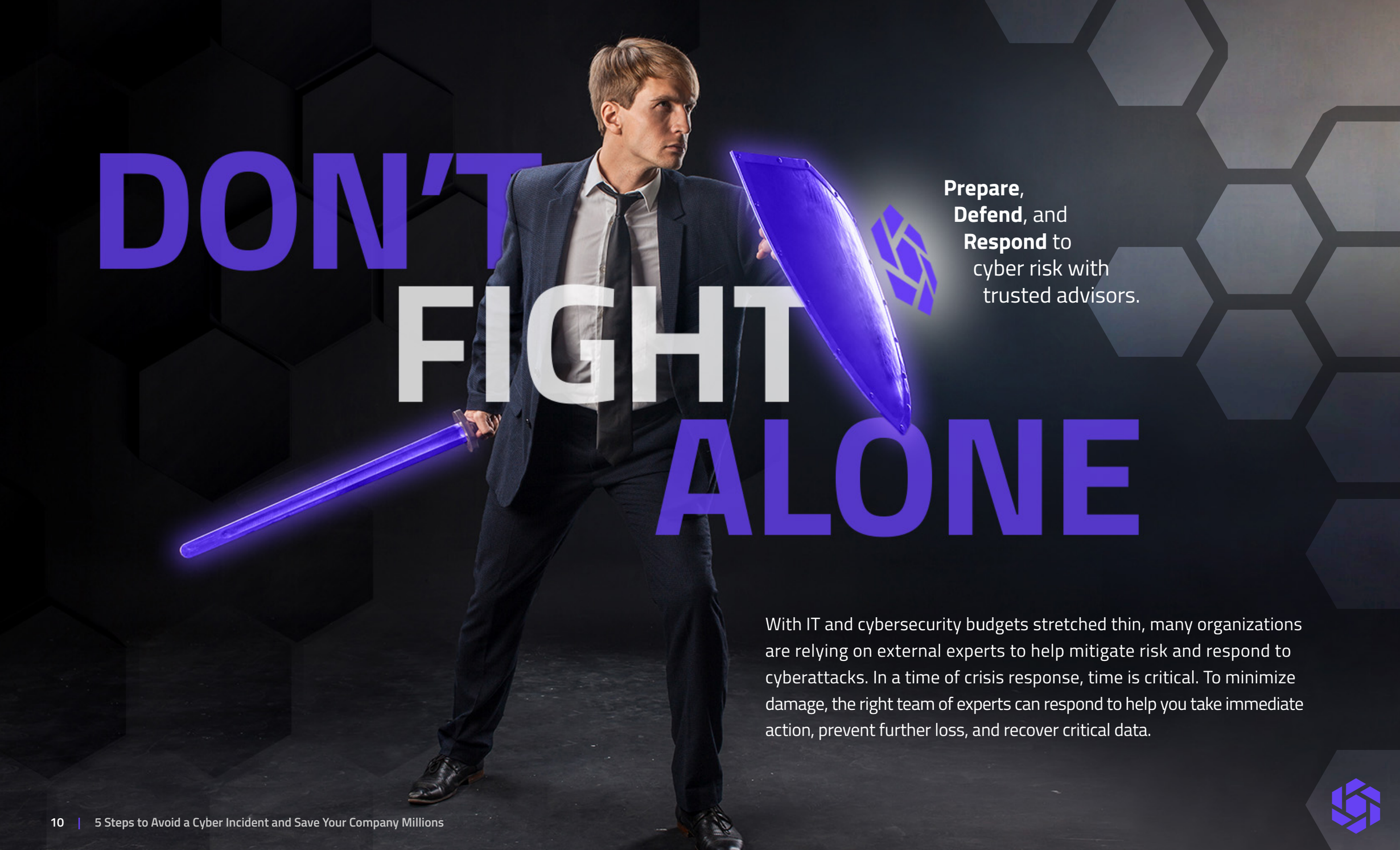
EXTERNAL RISK ANALYSIS

Conducting an analysis of your external exposure and gaining an adversarial point of view is critical to understanding where your biggest risks lie and what is in your control to close them. By identifying potential attack vectors and vulnerabilities, you can develop a proactive strategy to strengthen your defenses and minimize the impact of a potential breach.

CYBER AWARENESS TRAINING

It's estimated that roughly 88% of data breaches[1] are caused by a mistake made by an employee. As a result, it's essential to raise awareness among employees and other stakeholders about potential risks and threats. By helping them recognize and respond to these threats, they will be better equipped to defend themselves and your organization.

1. "The Psychology of Human Error," Tessian, 2020



DON'T FIGHT ALONE

Prepare, **Defend**, and **Respond** to cyber risk with trusted advisors.

With IT and cybersecurity budgets stretched thin, many organizations are relying on external experts to help mitigate risk and respond to cyberattacks. In a time of crisis response, time is critical. To minimize damage, the right team of experts can respond to help you take immediate action, prevent further loss, and recover critical data.

HOW SECURITYSCORECARD CAN HELP

About SecurityScorecard's Cyber Resilience Services

SecurityScorecard Cyber Resilience Services help organizations build, defend, and strengthen cybersecurity and third-party risk management programs. Our Cyber Resilience Services team brings 100+ years of collective experience in cybersecurity investigations across government and private sectors with specialties in Digital Forensics, Incident Response, Penetration Testing, Red Teaming, Tabletop Exercises, and Third-Party Risk Development.

Through the acquisition of LIFARs in 2022, SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident responses, providing a 360-degree approach to security. Cyber Resilience services are enriched by SecurityScorecard's ratings and its Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team. By employing Attack Surface Intelligence (ASI), Cyber Risk Intelligence, and ratings on every engagement, SecurityScorecard empowers organizations to respond to and defend against cyber threats.

SERVICES

Digital Forensic and Incident Response

Be ready to respond to any threat confidently and mitigate business interruptions from a cyberattack by partnering with industry-leading experts in digital forensic and incident response services. Integrate data forensics and incident response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard on demand.

Proactive Security

Defend your organization with a range of proactive services, including: penetration testing, red teams, and tabletop exercises. Battle-test your security controls, identify gaps in your attack surface, and enhance your ability to defend against cyberattacks.

Cyber Risk Intelligence

Gain clarity to proactively eliminate cyber risk with customized, actionable threat intelligence about emerging and active threats specific to your organization. Delivered by SecurityScorecard's STRIKE Threat Intelligence team, Cyber Risk Intelligence fills critical intelligence gaps and illuminates cyber risk trends, enabling cyber security teams to deploy limited cyber resources to the most efficient areas.

Third-Party Risk Management Program Development

Build and optimize your Third-Party Risk Management program by partnering with our subject matter experts to reduce your overall risk across your entire vendor ecosystem. We'll partner with you to align people, processes, and technologies to mature your current business ecosystem risk management program or build a new one.

Score Guarantee

Risk reduction strategies informed by SecurityScorecard will deliver meaningful returns on investment. By maintaining an "A" rating, your organization shows that cyber resilience is its priority. With Score Guarantee, customers with an "A" rating who experience a cyber incident are eligible for complimentary incident response services.

Enterprise Cyber Risk Management Program Development

Reduce your attack surface and alleviate future risks with SecurityScorecard's multi-prong enterprise cyber risk management solution. Partner with SecurityScorecard to continuously monitor your security posture against your peers, track assets, discover vulnerabilities and threats in your attack surface, turn deep contextual knowledge into action, and verify your cyber defenses are effective and resilient.

PRODUCTS

Security Ratings

Consistent and data-driven cybersecurity ratings enable our customers to understand the vulnerabilities in their own environment as well as their third and fourth parties. A standard A-F grading scale streamlines cyber risk communication and empowers risk mitigation across the entire vendor ecosystem. These ratings are becoming a trusted barometer of cyber resilience because they provide a standard unit of measurement and transparency. With this common language and level of insight, organizations can identify their own vulnerabilities in addition to the cyber risks posed by their suppliers and make informed decisions to strengthen their cyber defenses.

Security Assessments

SecurityScorecard's security assessments provide a streamlined approach to validating and assessing vendors at scale. With the help of automation and machine learning, organizations are able to shorten the process, save time, and gain a 360-degree view of vendors with the only customizable questionnaire to automatically validate responses against cybersecurity hygiene.

Cyber Risk Quantification

Cyber risk is no longer just an IT problem. Holistic conversations about the financial impact of cyber risk are needed to ensure the sustainability of the business. Start using cyber risk quantification to drive risk management strategies and translate cyber risk into dollars.

Attack Surface Intelligence (ASI)

Most threat hunters find it challenging to stay up to date on current threats as adversaries become more sophisticated and the global attack surface continuously evolves. ASI aids threat hunters in collecting thorough and essential data on the global attack surface for faster, more effective risk mitigation and threat prioritization.

Automatic Vendor Detection (AVD)

Security and third-party risk management teams are struggling to keep up with the growing ecosystems of third- and fourth-party vendors supporting their business. AVD instantly gives you a view of your entire business ecosystem, enabling you to visualize and take active steps to mitigate risk.

Watch List

With Watch List, organizations can add any company to a list to continuously monitor scores only and still have the flexibility to add those companies to a portfolio for a more detailed look at potential issues and remediation prioritization should a risk arise.

Marketplace

Security, IT, and VRM teams deploy an average of 47 different cybersecurity technologies and solutions, and many don't integrate with each other. The SecurityScorecard Marketplace helps you maximize and integrate investments in your security stack with out-of-the-box integrations with leading technology organizations, and the ability to build your own custom solutions with our Rule Builder and SecurityScorecard's APIs. Integrate SecurityScorecard data into your tech stack to drive integrated workflows, mitigate risk faster, and augment security data through our ecosystem of 60+ integrations, apps, and digital risk intelligence data.

SecurityScorecard Academy

Up-level internal stakeholders with certifications and knowledge to augment your security program, with courses ranging from cyber insurance, board reporting, third-party risk management, and more. We give your team the products to fill knowledge gaps and gain the skills they need to take control of your organization's cybersecurity

Reporting Center

Effectively communicate your cybersecurity strategy and risk posture to the Board and C-Suite in an easy-to-understand ratings language. Align cybersecurity with business needs, report on your organization's performance, and demonstrate the efficacy and ROI of your cybersecurity programs.

About SecurityScorecard

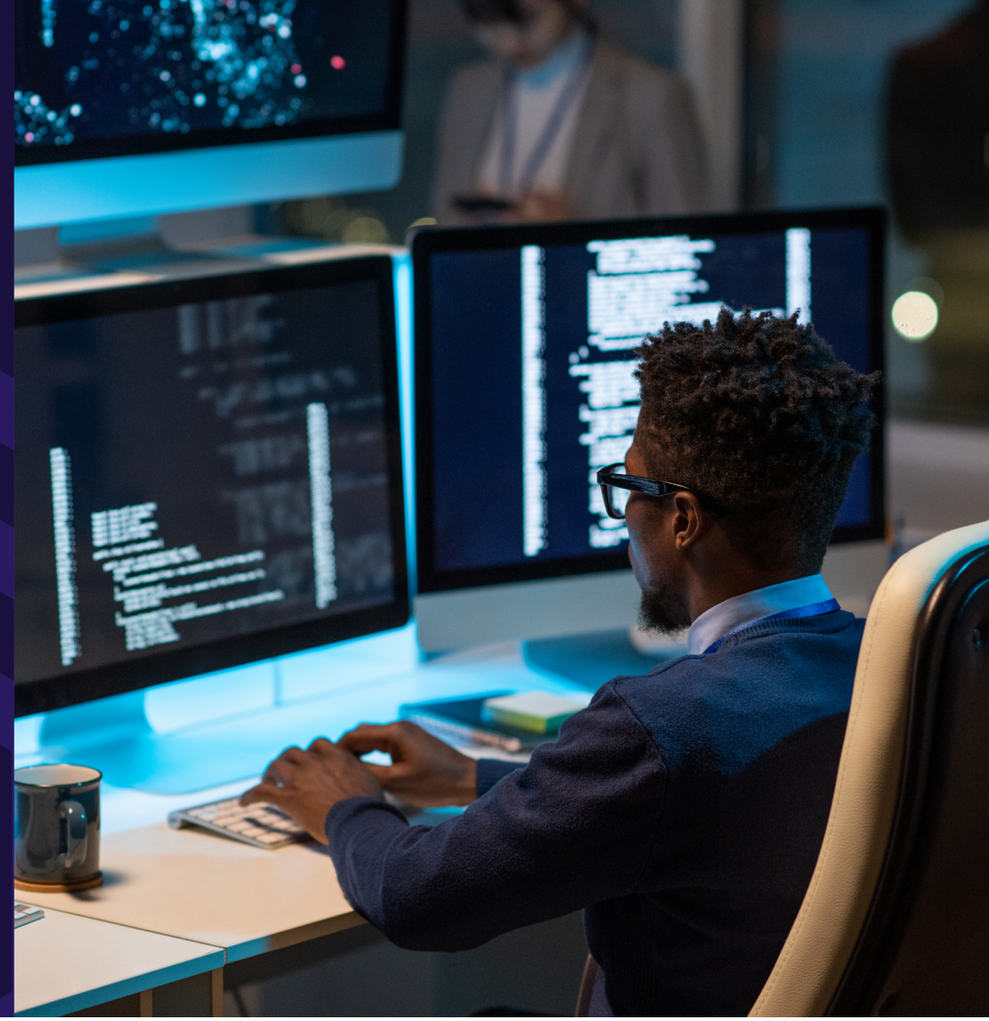
Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

About STRIKE

SecurityScorecard's STRIKE Threat Research, Intelligence, Knowledge, and Engagement team is an elite team of cyber security experts with over 100 years of collective experience in cyber security investigations and research. STRIKE Team members come for varying backgrounds, including experience with intelligence services, special operations units, and Fortune 50 cyber threat intelligence teams.



Talk to an Expert

Prepare, defend, and respond to cyber risk with trusted advisors.

GET STARTED

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com
United States: (800) 682-1701
International: +1(646) 809-2166

5 Steps to Avoid a Cyber Incident and Save Your Company Millions

Cheat Sheet

SecurityScorecard

STEP 1
Set a cybersecurity budget

- [ ] Conduct an inventory of your cyber defense tools
- [ ] Assemble an incident response team (either in-house or external)
- [ ] Cost our Required proactive measures and services for the year
- [ ] Invest in cyber insurance

STEP 2
Assess your incident response team's capabilities

- [ ] Assess your team's incident response capabilities, such as:
  - Incident detection and identification
  - Containment and eradication
  - Recovery and restoration
  - Post-incident analysis and reporting
- [ ] Identify any gaps or weaknesses in your response readiness
- [ ] Inquire about your digital forensics firm's standard operating procedures (SOPs)

STEP 3
Define your incident response plan

- [ ] Create an incident response plan (IRP)
- [ ] Collaborate with key stakeholders in building the IRP
- [ ] Define key steps for responding to a cyber incident: contain, investigate, respond, and report
- [ ] Establish clear channels of communication

STEP 4
Evaluate your cyber insurance policy

- [ ] Understand the type of coverage being provided
- [ ] Know how the premium is calculated and what kind of incidents are covered
- [ ] Find out the deductible and maximum coverage amount
- [ ] Determine if the policy covers digital forensics and incident response
- [ ] Find out if clauses are included that trigger additional sub-limits or coverage exclusions
- [ ] Ask if the policy covers lost sales or downtime due to a ransomware attack (and if extortion payments are covered)
- [ ] Determine if your cyber insurer chooses the incident response companies or if you do
- [ ] Find out if your cyber insurer handles rein-statements of coverage in the event of a claim

STEP 5
Consider implementing proactive services

- [ ] Penetration Tests
- [ ] Vulnerability Management
- [ ] Tabletop Exercises
- [ ] Red Team
- [ ] Security Assessments
- [ ] Threat Hunting
- [ ] External Risk Analysis
- [ ] Threat Intelligence
- [ ] Cyber Awareness Training

Want to Learn More?
Talk to an Expert.

GET STARTED