Cyber GRX

Third-Party Cyber Risk Intelligence:

Where and Why Your Organization Needs It

Table of Contents

Introduction

The digital transformation of business systems and processes has created countless opportunities for organizations when it comes to scale and sustainability. The great migration to cloud-based services and platforms has allowed organizations to tap into new markets, drive down costs, and improve efficiencies. However, this migration has also created several new cyber risks that must be managed.

The impact that cyber threats have on organizations has continued to evolve as the number of cyberattacks has increased year over year. But cyber risk within the organization is no longer the responsibility of security and risk management teams alone. In today's landscape, cyber risk has become a business-wide concern that requires a coordinated response from all parts of the organization.

Minimizing Attack Surfaces In and Outside Your Organization

When it comes to cyber risk, one of the most important steps an organization can take is to minimize its attack surface. An attack surface is simply the number and variety of potential entry points an attacker could use to access a system or network. The more entry points there are, the easier it is for an attacker to find a way in.

This is why organizations need to take a holistic approach to security, looking at the systems and networks that need to be protected and the people, processes, and technologies involved.

Understanding Today's Internal and External IT Risks

To understand the importance of minimizing attack surfaces, it's first essential to understand the different types of cyber risks an organization faces.

Internally, organizations face various cyber security challenges when properly implementing IT-related processes and technologies. These challenges can include:

- Misconfigured systems that are susceptible to attack
- Lack of or incorrect patch management
- Inadequate cyber training programs for employees
- Insufficient disaster recovery planning

While many organizations work to identify and address these risks as quickly as possible, risks that originate outside the organization can be more challenging to diagnose and even harder to mitigate.

As organizations extend their infrastructures and do business with more external third-party providers, the number of potential attack vectors increases. This is because as an organization adds more systems and applications, it also adds more points of vulnerability. External cyber risks can include:

- Third-party providers with outdated security protocols
- Unsecured cloud storage services
- Malicious insiders
- Compromised systems and networks of business partners or suppliers

While both internal and external cyber risks can be successfully mitigated with the right approach, identifying all of your organization's risks is the most critical first step.

Establishing Best Practices for Reducing Exposure

A large part of mitigating cyber risk is establishing best practices for reducing your organization's exposure. This means implementing measures to protect your internal systems, networks, as well as your third-party providers and solutions. One key area of focus should be minimizing the attack surface by disabling unused features, closing loopholes, and hardening systems against infiltration.

Adopting a risk-based approach is also critical, as it will allow you to prioritize areas of concern and allocate resources accordingly. By taking a holistic view of your organization's security posture, you can identify potential weak points and address them before they become a problem.

Using the Right Tools and Solutions to Combat Security Threats

To combat security threats effectively, you need the right tools and solutions. This includes a combination of people, processes, and technologies that can help you identify and mitigate cyber risks.

One of the most important tools you can have at your disposal is a comprehensive risk management solution. A good risk management solution can help you identify and assess potential threats, prioritize areas of concern, and take action to mitigate risks.

Third-party providers and solutions are another critical part of your overall business strategy, and it's important to select the right ones. It's crucial to vet these providers carefully and ensure that they meet not only your business needs but also your specific security, performance, and reliability requirements. Since not all providers are created equal, it's also essential to actively monitor their performance and take corrective action if necessary. Utilizing platforms that help you track your internal and external cyber risk factors can help you do this effectively.

Why Understanding Third-Party Cyber Risk is Important for Organizations

82%

of companies said that third-party threats present the most significant risk of exposure

67%

of companies said they experienced at least one third-party related cyber incident in the past year

LESS THAN 50%

of companies actively prioritize third-party risk management strategies

41%

the amount of critical data that will be shared with third-parties in five years

Data from CyberGRX survey done in conjunction with **Forrester Consulting**

Diversifying Procurement Processes to Maximize Security

For modern businesses, procurement teams have the difficult challenge of balancing business security needs with the need to find efficiencies and cost savings in the procurement process, as well as accelerating the onboarding of new vendors. This creates a heightened risk for cyberattacks, as hackers can access valuable data and systems through third-party providers.

Without understanding all of the risks associated with a supplier relationship, companies can find themselves in difficult situations down the road that not only impact their ability to operate efficiently but can also leave them open to security concerns and compliance issues. This makes it critical that businesses implement the right tools and solutions for their procurement teams to make smarter purchasing decisions from qualified vendors.

To reduce the risk of cyberattacks, it is more important for procurement teams to diversify their third-party ecosystem while also making business security and viability decisions.

Recognizing the Need for Safer Procurement Practices

One of the first steps in improving procurement practices is recognizing the need for better security. More businesses have become more aware of the risks posed by cyberattacks in recent years, and many are now taking steps to improve their cybersecurity posture.

A recent study by **Forrester Consulting** found that 67 percent of organizations experienced a third-party risk incident in the last year. These statistics continue to increased year over year, and it's clear that businesses are struggling to keep up with the latest threats.

Procurement teams play a much more critical role than ever before in safeguarding businesses from cyberattacks, and their involvement and collaboration with other security-minded stakeholders in the organization are critical. By partnering with risk management and security teams, procurement professionals can better understand what they should be looking for when establishing relationships with third-party vendors.

Using Point In Time Assessments to Minimize Cyber Risks

For any individuals responsible for procuring goods and services for the company, it's essential to be aware of the potential risks involved in doing business online. Cybercriminals are always looking for new ways to exploit vulnerabilities, and they are becoming increasingly sophisticated in their attacks. As a result, procurement teams must take analytical steps to minimize their exposure to cyber risks.

The most common way to do this is by conducting a point in time assessment. This type of assessment provides a snapshot of an organization's security posture at a specific moment in time. By understanding the current security posture while measuring trends over time, procurement teams can make informed decisions about how they contribute to a more secure organization.

While performing assessments has a value in understanding third-party risk, an approach that includes third-party cyber risk intelligence to monitor and track risk exposure across all attack surfaces over time will provide a more accurate and near-real-time view of your risk posture. Collecting and organizing this information in one unified platform gives procurement teams access to real-time and historical information that can be used to drive safer purchasing decisions and a more proactive approach to third-party risk mitigation.

Increasing Visibility and Control For Security Professionals

It is becoming more and more critical for security professionals to have visibility and control across all attack surfaces. This includes your organization's third-party ecosystem, which can be a significant source of risk if not managed properly.

Many organizations struggle with this, as they are often unable to get a clear view of all the devices and systems that make up their extended network. This makes it challenging to identify and mitigate these systems' potential risks. One way to help solve these issues is by creating a unified view of your organization's internal and external risk factors.

Creating a Single Source of Truth

To combat security threats effectively, you need the right tools and solutions. This includes a combination of people, processes, and technologies that can help you identify and mitigate cyber risks.

One of the most important tools you can have at your disposal is a comprehensive risk management solution. A good risk management solution can help you identify and assess potential threats, prioritize areas of concern, and take action to mitigate risks.

Third-party providers and solutions are another critical part of your overall business strategy, and it's important to select the right ones. It's crucial to vet these providers carefully and ensure that they meet not only your business needs but also your specific security, performance, and reliability requirements. Since not all providers are created equal, it's also essential to actively monitor their performance and take corrective action if necessary. Utilizing platforms that help you track your internal and external cyber risk factors can help you do this effectively.

Assessing and Enforcing Security Standards at Scale

Another vital way to improve your organization's security posture is by assessing and enforcing security standards on a larger scale. However, this can be increasingly difficult as an organization expands its operations and engages with multiple third-party vendors.

To enforce high-security standards, especially when managing compliance with partners outside of your organization, security teams need access to actionable data insights regarding direct or indirect risks associated with third-party networks. This data can then be applied to a data set that includes a risk-based assessment framework to help your team decide which systems and vendors to engage with and how best to protect your organization from potential threats.

However, it's important to remember that no one solution can provide complete security. As such, security teams must adapt their strategies as their organization grows and changes continuously. This is where having more real-time data, such as threat intelligence, provides additional value to collected assessments. By using the right combinations of tools and techniques, they can ensure they aren't missing any potentially dangerous trends and address any risks before they have a chance to cause harm.

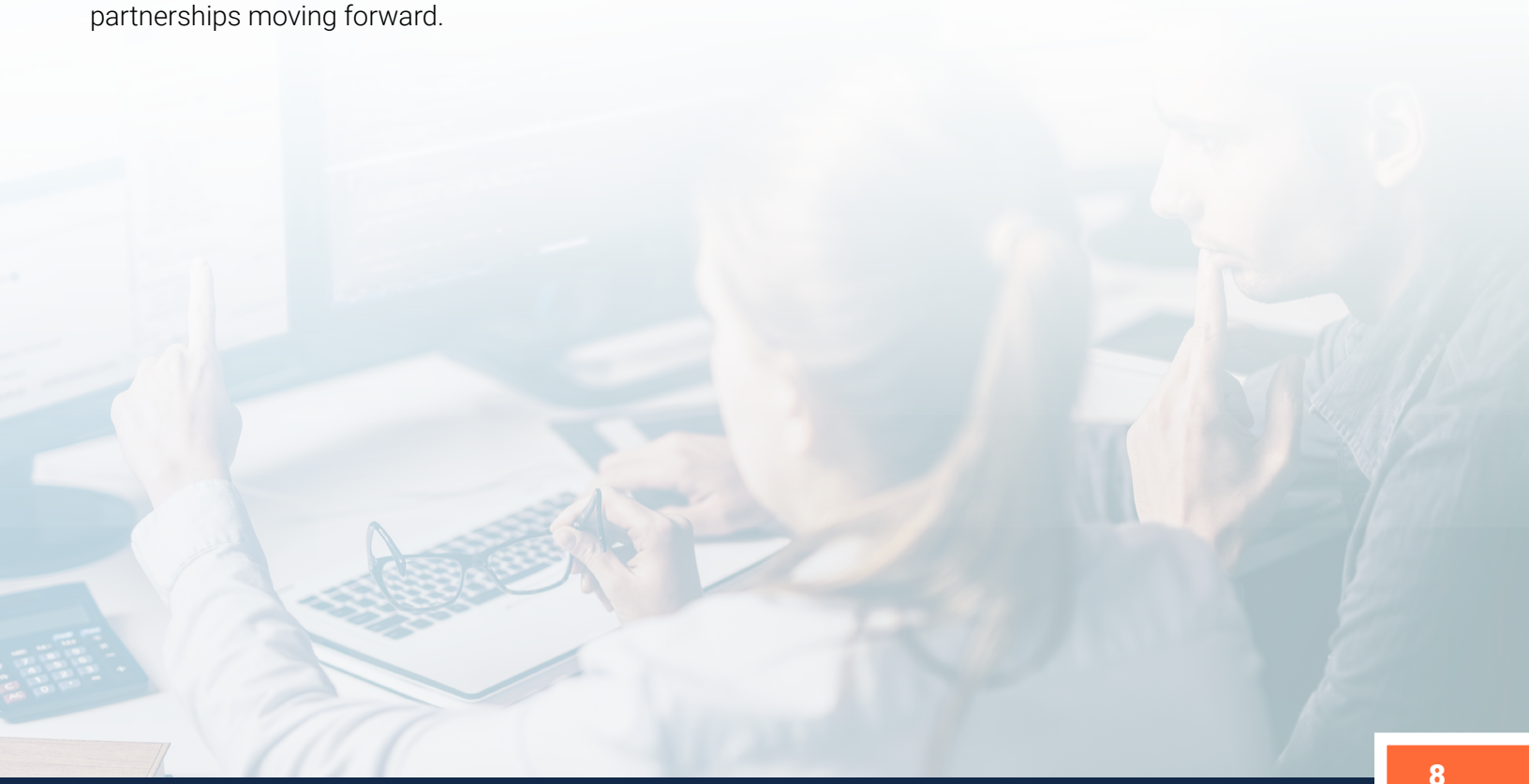
Moving From Reactive Use to Proactive Use of Third-Party Cyber Risk Intelligence

The security industry has traditionally been reactive in its approach to third-party risk. However, this reactionary mindset is no longer appropriate in the face of the current threat landscape. Instead, security teams need to be proactive in their collection and use of third-party cyber risk intelligence.

Third-party cyber risk intelligence is the process of identifying, assessing, and managing risks to an organization's information security. It involves using a variety of data sources to identify potential threats and vulnerabilities that could impact the organization's cybersecurity posture. These sources can be associated with the technology and infrastructure that a business uses to support its operations as well as external partnerships that are relied on to scale its resources, products, and services.

Third-party cyber risk intelligence gives organizations the ability to visualize their risk exposure outside the boundaries of their own operating environment. Today, many organizations rely heavily on third-party vendors to provide critical services, such as cloud hosting or software development, so it is essential to understand these vendors' risks. Third parties may have vulnerabilities that could be exploited, and they may also have access to your organization's sensitive data.

By utilizing third-party cyber risk intelligence, organizations can get away from reactive security processes that put their business at high risk and instead incorporate a more proactive approach towards reducing the attack surfaces. Third-party cyber risk management platforms like CyberGRX enable security teams to have a more complete view of their entire portfolio of third parties, giving them the ability to see not only attested assessment responses but additional data insights including predicted assessment responses and coverage of controls commonly exploited in cyber threats. This added transparency reduces the potential of costly disruptions to mission-critical operations and better informs stakeholders on how to choose the right partnerships moving forward.



Making Data-Driven Decisions Around Risk Management

Risk management teams in modern businesses have the difficult challenge of understanding and navigating all forms of risk inside and outside of their organization. However, with more organizations expanding their digital footprints across multiple third-party providers and solutions, cyber security risks are taking a more critical role, and many find it challenging to get a real sense of their overall cyber risk exposure.

Cyber risk management platforms are one of the many tools risk management teams can use to help them make data-driven decisions about their overall risk posture. By aggregating and analyzing data from both internal and external sources, risk management platforms can provide organizations with a comprehensive view of their cyber risks while giving them the ability to mitigate them successfully.

Establishing a Risk-Based Approach to Decision Making

A risk-based approach is recommended for all organizations, but it's especially critical for businesses with a complex cyber risk profile. By understanding the different types of risks an organization faces and how those risks interact with one another, risk management teams can make better decisions about where to focus their resources. Adopting a risk-based approach to decision-making also allows businesses to prioritize their most critical risks and take steps to mitigate them.

One of the first steps to creating a risk-based approach is understanding an organization's risk appetite. This means understanding how much risk the business is willing to take on and what risks it is not comfortable accepting. Once this is understood, the next step is to create a risk management strategy that aligns with the company's overall business objectives.

Third-party cyber risk management solutions can help organizations by providing them with the data they need to make informed decisions about their cyber risk posture and ensure decisions made support the company's acceptable risk level.

Prioritizing Your Mitigation Strategies

Not all risks are created equal when it comes to mitigating cyber risks. As a result, organizations need to prioritize their mitigation strategies to protect themselves from the most severe threats.

Third-party cyber risk intelligence can help organizations do just that by providing information about the specific threats they face and how likely they will occur. Armed with this information, businesses can focus their resources on mitigating the most severe threats first, which will help reduce their overall risk exposure.

When prioritizing mitigation strategies, it's important to remember that not all risks can be mitigated. In these cases, businesses need to develop a plan for responding if and when a risk event occurs. For example, it's crucial to have a plan for how the business will respond to a data breach through engagement with a third-party vendor. This may include incident response plans, data loss prevention (DLP) policies, and other security measures.

Making Data-Driven Decisions to Improve Your Risk Posture

Third-party risks are a significant concern for organizations working with cloud-based services and vendors. Unfortunately, many companies don't have the visibility into their third-party networks that they need to understand and manage these risks. This lack of visibility can lead to significant security vulnerabilities and data breaches.

Third-party cyber risk intelligence is essential for understanding and managing these risks. With the actionable insights provided, organizations can make data-driven decisions about where to focus their resources and how to improve their risk posture. By identifying and addressing vulnerabilities in their third-party networks, organizations can reduce the chances of a data breach or other security incident. By collecting and analyzing cyber risk intelligence, organizations can better understand their specific risks and vulnerabilities while giving them the information they need to make the right business decisions at the right time.

Conclusion

Regardless of the industry or organization size, all companies face some level of cyber risk. And with the number of data breaches increasing every year, it's more important than ever for organizations to have visibility into their cyber risk exposure and take steps to mitigate it. However, while the importance of cyber risk intelligence is evident, many organizations still struggle with the ability to collect and interpret the data they need to make informed decisions about their risk exposure, especially across all of their third-party relationships.

Thankfully, CyberGRX has developed the industry's first and only platform that provides complete, near real-time visibility into an organization's entire third-party cyber risk exposure. By aggregating data from multiple sources and applying advanced analytics, CyberGRX gives organizations the ability to see all of their third-party risks in one place and the data to decide how to mitigate them.

Whether helping security teams minimize their attack surfaces, giving procurement specialists the insight they need to make smarter purchasing decisions, or providing risk management professionals the visibility they need to reduce their exposure to cyber incidents, CyberGRX is changing how organizations think about and manage their third-party cyber risk.

If you're looking for better visibility and control over your cyber risk posture in relation to third parties while also reducing the cost and complexity of your third-party risk management protocols, schedule a demo today to see how CyberGRX can help you take back control over your risk exposure.