



NEVER TRUST, ALWAYS VERIFY

**ADDRESSING THIRD-PARTY CYBER RISK EXPOSURES
IN THE ERA OF AUTOMATION**

TABLE OF CONTENT

01

Executive Summary

02

Introduction

- A. The evolving landscape of third-party relationships.
- B. The rise of automation in business processes.
- C. The intersection of third-party risk and automation.
- D. The role of IOT in the Supply Chain.

03

Understanding Third-Party Cyber Risk

- A. Definition and scope.
- B. Common types of third-party cyber risks.
- C. The impact of third-party breaches on organizations.
- D. Assessing Trust in Your Business Ecosystem.
- E. Impact of Supply Chain Attacks/Incidents.

04

The Era of Automation: Opportunities and Challenges

- A. Benefits of automation in business processes.
- B. Digital Trust: Revolutionizing Cybersecurity Through AI.
- C. Increased reliance on third-party services and technologies.
- D. New risk vectors introduced by automation.
- E. Bringing it all together: Security risks at the Intersection of IoT and Automation in the Supply Chain.

05

Current Approaches to Third-Party Risk Management

- A. Traditional manual assessment methods.
- B. Limitations of manual approaches in the digital age.
- C. The need for a paradigm shift.

06

Leveraging Automation for Third-Party Cyber Risk Management

- A. Continuous monitoring and real-time risk assessment.
- B. Automated due diligence and vendor onboarding.
- C. AI-driven predictive risk analytics.
- D. Automated policy enforcement and compliance checking.

07

Key Components of an Automated Third-Party Risk Management Program

- A. Asset discovery and inventory management.
- B. Vulnerability scanning and threat intelligence integration.
- C. Automated risk scoring and prioritization.
- D. Workflow automation for risk mitigation and incident response.
- E. Integration with existing security and GRC platforms.

08

Best Practices for Third-Party Risk Management

- A. Our Recommendation.

09

References and Additional Resources

- About DigitalXForce.
- Our Solutions.



Executive Summary

Organizations of all sizes are becoming increasingly reliant on third-party vendors, partners, and service providers to drive innovation, efficiency, and growth in today's interconnected business ecosystem. However, the expanded network of relationships has introduced new and complex cyber risk exposures that traditional risk management approaches struggle to address effectively.

This whitepaper explores the critical intersection of third-party cyber risk management and automation, offering insights into how organizations can leverage automation to enhance their security posture, streamline risk assessment processes, and stay ahead of evolving threats. By embracing automation, businesses can transform their third-party risk management program, moving from periodic, manual assessments to continuous, real-time monitoring and mitigation strategies.



Key takeaways from this whitepaper include:

- Understanding the evolving landscape of third-party cyber risks in the era of automation.
- Exploring the limitations of traditional risk management approaches and the need for a paradigm shift.
- Understanding the revolution of Cybersecurity with Digital Trust through AI.
- Identifying key components of an automated third-party risk management program.
- Providing practical guidance on implementing and optimizing automated risk management strategies.
- Examining real-world case studies and best practices for success.

As organizations navigate the complexities of digital transformation and an ever-expanding threat landscape, the ability to effectively manage third-party cyber risk exposures will be crucial for maintaining resilience, trust, and competitive advantage in the digital age.



A.

The evolving landscape of third-party relationships

In recent years, the business world has witnessed a dramatic shift in how organizations operate and collaborate. The rise of cloud computing, software-as-a-service (SaaS) platforms, and specialized service providers has led to an unprecedented level of interconnectedness between companies.

This ecosystem of third-party relationships has become essential for driving innovation, improving operational efficiency, and achieving scalability in today's fast-paced business environment.

From IT infrastructure and data processing to customer service and supply chain management, organizations are increasingly outsourcing critical functions to third-party vendors. This trend has accelerated even further in the wake of the global pandemic, as remote work and digital transformation initiatives have pushed companies to adopt new technologies and services at an unprecedented rate.

Innovation in the digital transformation era relies on interconnected systems and expansive technological ecosystems. Organizations' software development and digital service delivery to both external and internal customers are deeply intertwined with third-party partnerships. The innovation supply chain frequently incorporates these key external resources:

1. Cloud infrastructure and hosting services.
2. Software-as-a-Service (SaaS) solutions.
3. Open Application Programming Interface (API) integrations.
4. Third-party software libraries and components.
5. Specialized technical consulting.
6. Data aggregation and analytics services.
7. Managed IT services.

While these third-party relationships offer numerous benefits, they also introduce significant risk management and cybersecurity challenges. Each new connection to a third-party system or service represents a potential entry point for cyber threats, expanding the attack surface and increasing an organization's overall risk profile.

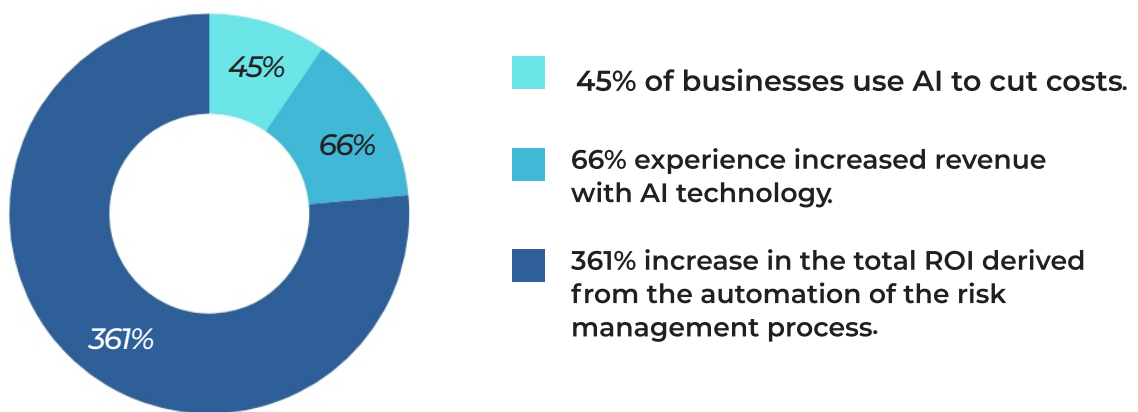
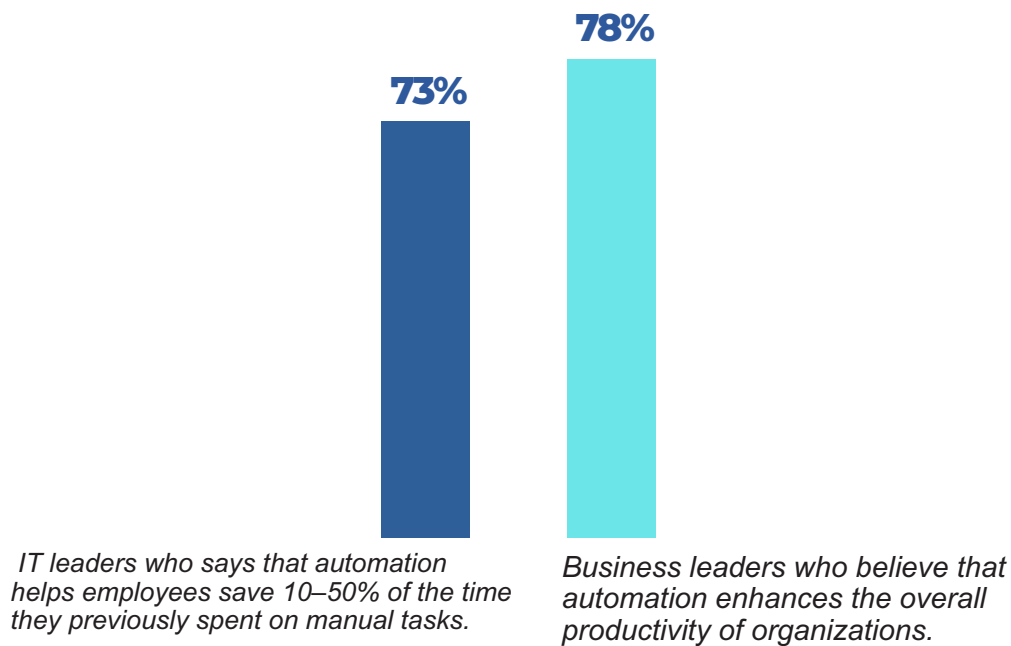
B.

The rise of automation in business processes

Parallel to the growth of third-party relationships, we've seen a surge in adopting automation technologies across various business functions. Robotic Process Automation (RPA), Artificial Intelligence (AI), and Machine Learning (ML) are being deployed to streamline operations, increase efficiency, and reduce human error in a wide range of processes.

80%

of businesses are speeding up process automation, while **50 percent plan to automate all repetitive tasks.**



Automation is transforming everything from customer service chatbots and marketing campaigns to supply chain logistics and financial transactions.

This shift towards automated processes has enabled organizations to operate at unprecedented scales and speeds, handling vast amounts of data and transactions in real time.

However, the rapid adoption of automation also introduces new challenges and potential vulnerabilities. Automated systems can potentially amplify the impact of errors or security breaches, and the complex interplay between various automated processes can create unforeseen risks and dependencies.

C. The intersection of third-party risk and automation

At the convergence of these two trends – the proliferation of third-party relationships and the rise of automation – lies a new frontier in cybersecurity and risk management. Organizations now face the dual challenge of managing an expanding network of third-party risks while also navigating the complexities introduced by automated systems and processes.

This intersection creates both opportunities and challenges. On one hand, automation technologies offer powerful new tools for monitoring, assessing, and mitigating third-party risks at scale. On the other hand, the increased reliance on automated systems and third-party services creates new attack vectors and potential points of failure that must be carefully managed.

D. The role of IoT in the Supply Chain

IoT transforms supply chains with real-time tracking, predictive maintenance, and automation. Smart sensors, RFID, and GPS enhance visibility, optimize inventory, and streamline logistics. Industrial IoT prevents downtime, while AI-powered forecasting improves efficiency.

However, increased connectivity introduces cybersecurity risks, making robust security essential for resilient, connected supply chain operations.

A. Definition and scope

Third-party cyber risk refers to the potential threats and vulnerabilities introduced to an organization through its relationships with external entities such as vendors, suppliers, partners, and service providers. These risks arise from the interconnected nature of modern business operations, where organizations often share data, systems, and network access with third parties to facilitate various business functions.

The scope of third-party cyber risk is broad and encompasses:

- 1 **Data loss resulting from inadequate security measures at a third-party vendor.**
- 2 **Disruptions to critical services due to cyber incidents affecting third-party providers.**
- 3 **Compliance violations stemming from a third party's failure to adhere to regulatory requirements.**
- 4 **Reputational damage caused by data breach at associated third parties.**
- 5 **Financial losses due to fraud or theft propagated through third-party connections.**

It's important to note that third-party risk extends beyond immediate vendors to include fourth-party and even fifth-party relationships, creating a complex web of potential vulnerabilities that organizations must navigate as part of supply chain risk management.

While organizations can delegate IT functions and outsource operations, they retain the accountability for Cybersecurity risk management. This fundamental principle underscores the critical nature of third-party risk management.

Critical infrastructure breaches through third-party vendors can paralyze entire communities. While compromised data typically draws public scrutiny to the primary organization, attacks on power grids, water systems, or transportation through vendor vulnerabilities can disrupt essential services and create cascading failures, making supply chain security a national security priority.

B.

Common types of third-party cyber risks

01

Data exposure

Third parties with access to sensitive data may inadvertently or maliciously expose this information, leading to data breaches.

02

Insecure APIs

Poorly secured Application Programming Interfaces (APIs) used for integration with third-party services provide an entry.

03

Supply chain attacks

Malicious actors may compromise a third-party vendor to gain access to multiple organizations in the supply chain.

04

Cloud security vulnerabilities

Misconfigurations or vulnerabilities in cloud services used by third parties can expose data or systems to unauthorized access.

05

Insider threats

Employees or contractors of third-party vendors may misuse their access privileges, intentionally or unintentionally causing security incidents.

06

Outdated or vulnerable software

Third parties using outdated or unpatched software can introduce vulnerabilities that attackers can exploit.

07

Inadequate access controls

Overly permissive access granted to third parties lead to unauthorized data access or system compromises.

08

Compliance failures

Third parties failing to meet regulatory requirements can expose organizations to legal and financial risks.

09

Operational disruptions

Cyber incidents affecting third-party service providers lead to business interruptions and financial losses.

10

Intellectual Property theft

Cybercriminals may target third parties to steal valuable intellectual property or trade secrets.

c. The impact of third-party breaches on organizations

The consequences of third-party cyber incidents can be severe and far-reaching:



Financial losses

Direct costs from incident response, legal fees, regulatory fines, and potential lawsuits can be substantial. Indirect costs from business disruption and lost revenue can also be significant.



Reputational damage

Security breaches involving third parties can erode customer trust and damage brand reputation, potentially leading to long-term business impacts.



Regulatory scrutiny

Organizations may face increased regulatory scrutiny and potential fines for failing to adequately manage third-party risks.



Operational disruptions

Cyber incidents affecting critical third-party services can lead to significant business disruptions and lost productivity.



Data loss

Breaches involving third parties can result in the loss of sensitive data, including customer information, intellectual property, and trade secrets.



Competitive disadvantage

Loss of intellectual property or strategic information through third-party breaches can impact an organization's competitive position.



Legal liabilities

Organizations may face legal action from customers, partners, or shareholders affected by third-party security incidents.



Increased security costs

Responding to and mitigating third-party incidents often requires significant investments in security measures and resources.



Loss of market share

Severe breaches can lead to customer churn and difficulty acquiring new customers, impacting market share.



Long-term strategic impacts

Repeated third-party incidents can force organizations to reassess their business models and partnerships, potentially leading to significant strategic shifts.



Impact on broader society

Critical infrastructure breaches through third-party vendors can paralyze communities. An attack on hospitals or utilities means life-support failures, power outages, and water contamination—turning cyber vulnerabilities into life-threatening emergencies.

Understanding these risks and their potential impacts is crucial for developing effective strategies to manage third-party cyber exposures in the era of automation.

As we move forward, we'll explore how automation technologies can be leveraged to address these challenges and strengthen an organization's overall security posture.

D. Assessing Trust in Your Business Ecosystem

How much of your business viability can you responsibly rely on unverified trust? Consider these critical questions about your vendors:

Cybersecurity Maintenance

Can you confidently assume that your most crucial vendors maintain a 90% or higher success rate in securing their internet-facing system software?

Threat Intelligence Focus

Do you have the assurance that all your vendors consistently direct their threat intelligence operations towards the most relevant internet points of presence that intersect with your organisation's critical operations and data flows?

Vulnerability Exploitation Risk

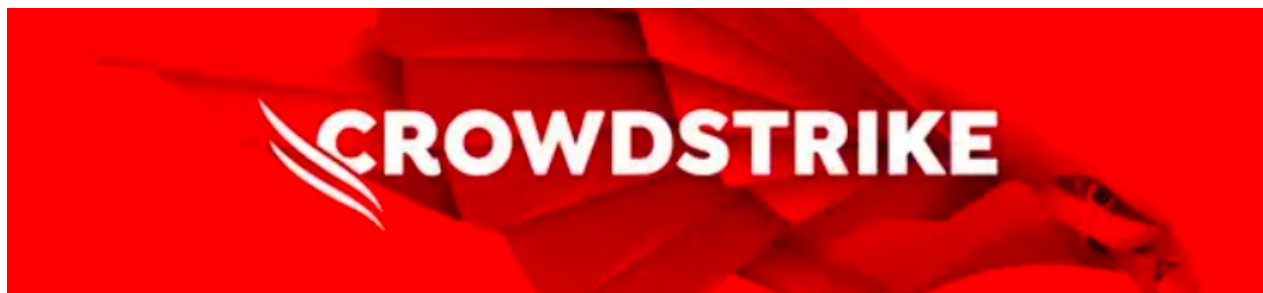
Can you be certain that vulnerabilities in your vendors' systems cannot be exploited to compromise systems housing your data?

E. Impact of Supply Chain Attacks/ Incidents

Supply chain attacks represent a particularly concerning category of multi-party cyber incidents. These events affect numerous organizations with both direct and indirect connections to the initial victim. Recent research indicates that ripple events can inflict financial damage up to 13 times greater than single-party incidents.

Several recent high-profile case studies illustrate the far-reaching consequences of third-party incidents:

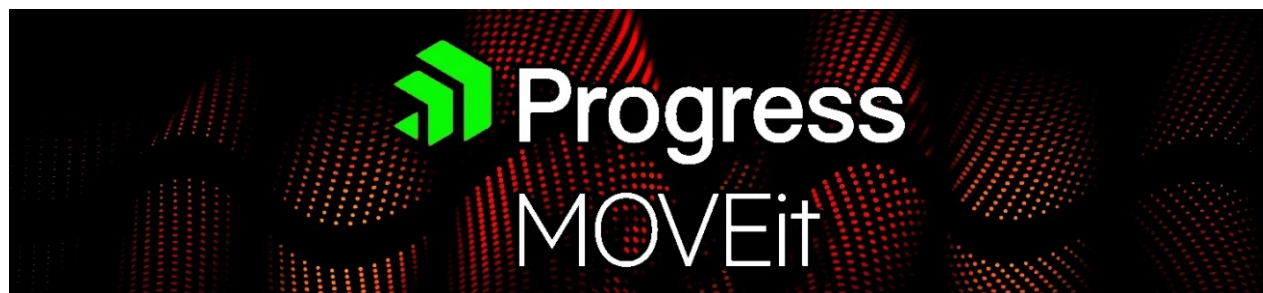
CrowdStrike Update



A global digital crisis unfolded in July 2024 as CrowdStrike's faulty update collided with Microsoft Windows systems, triggering worldwide IT failures. The buggy update, meant to enhance security, ironically undermined it instead. This wasn't a mere glitch, but a seismic event that exposed the fragility of our interconnected digital infrastructure. To be clear: this was not a cyber attack but a Cyber incident with a supply chain ripple effect.

The impact was staggering: major airports ground to a halt, with airlines like Delta, United, and American facing severe disruptions. From Sydney to Amsterdam, check-in counters resorted to manual processes. The financial sector reeled as banks and stock exchanges reported service interruptions. Even media outlets fell silent, unable to broadcast.

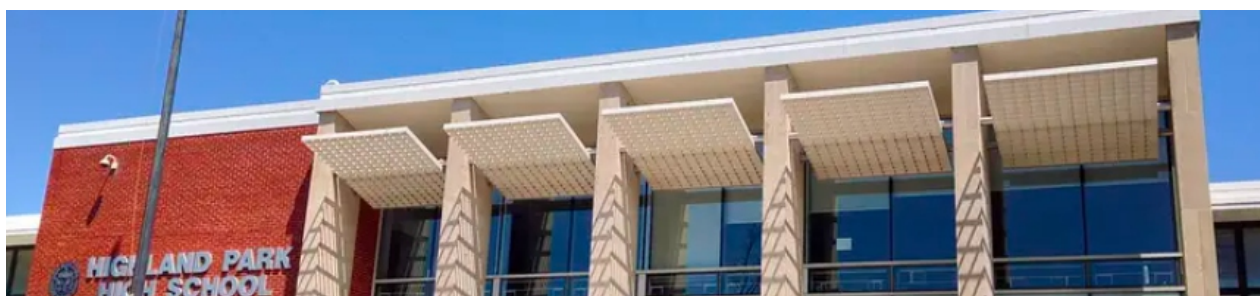
MOVEit



A major cyberattack on MOVEit, a managed file transfer software product, compromised thousands of organizations worldwide in 2023. The breach had wide-ranging consequences, affecting more than 2,600 organizations including major companies like the BBC, British Airways, Boots, and various government agencies - with Amazon now becoming the latest victim to disclose a breach.

That same year, researchers revealed that 97% of the UK's largest companies experienced supply chain breaches, with software supply chain attacks driving an 11% increase in financial losses compared to previous years.

US School Districts



Illuminate Education, a major provider of student-tracking software, fell victim to a cyberattack in 2022. The breach had far-reaching consequences, compromising data in the nation's two largest school systems - New York City Public Schools and Los Angeles Unified School District - along with numerous other institutions. That same year, Chicago Public Schools suffered a significant data breach affecting 495,000 student records, resulting from a breach at a third-party service provider.

Sargent & Lundy



A ransomware attack on Sargent & Lundy, a major US government contractor that designs power stations and handles nuclear security issues, compromised data from multiple electric utilities in October 2022. The breach was carried out by the Black Basta ransomware group and affected Sargent & Lundy, a company that has designed more than 900 power stations and thousands of miles of power systems. The company works with the Departments of Defense and Energy on nuclear deterrence projects.

Colonial Pipeline



Colonial Pipeline Company

A ransomware attack on Colonial Pipeline in May 2021, executed by the DarkSide group through a compromised VPN password, exposed critical vulnerabilities in America's infrastructure security.

The breach caused widespread disruption across the Eastern United States, triggering fuel shortages, panic buying, and price surges - leading the Transportation Security Administration to mandate new cybersecurity requirements for pipeline operators.

Change Healthcare:



UnitedHealth's Change Healthcare unit suffered a massive data breach in February 2024, affecting approximately 190 million Americans - nearly double initial estimates and marking the largest medical data breach in U.S. history.

The attack, carried out by the Russian ALPHV ransomware gang using stolen credentials, compromised sensitive information including Social Security numbers, medical records, and financial data, while causing months of nationwide healthcare system disruptions.

Solar Winds



The SolarWinds cyber incident of December 2020 marked a watershed moment in cybersecurity, exposing the vulnerabilities inherent in software supply chains. SolarWinds, a prominent provider of network and system monitoring software, fell victim to a sophisticated attack that compromised its Orion® platform.

The breach involved a complex, multi-stage malware program inserted into software updates. This malicious code exhibited advanced evasion techniques, disabling security tools and establishing covert connections to attacker-controlled servers. The malware remained undetected for months, highlighting the attackers' sophistication.

The impact was significant, but only a subset was directly targeted and compromised. An estimated 18,000 customers, including government agencies and 14% of Fortune 1000 companies, were affected. Even organizations not directly using SolarWinds products faced risks due to the company's pervasive presence in the tech ecosystem.

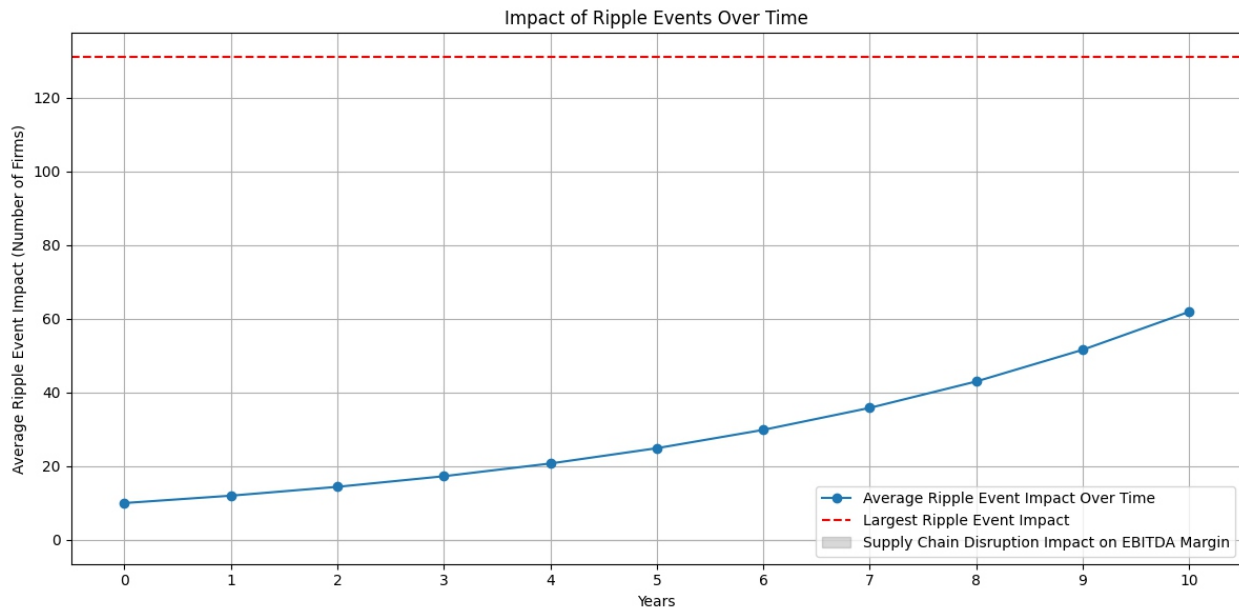
Financial repercussions were severe. Companies spent an average of \$12 million (11% of annual revenue) on incident response and forensics. Insured losses were estimated at \$90 million.

Toyota



Toyota, the world's largest auto manufacturer, faced an unprecedented production crisis triggered by a supply chain attack on one of its key suppliers in 2022. Kojima Industries, a manufacturer of plastic parts essential to Toyota's production line, fell victim to a sophisticated cyber intrusion.

The ripple effect was immediate and severe. Toyota was forced to halt operations across all 28 production lines in 14 of its domestic plants in Japan. This shutdown represented a staggering one-third of Toyota's global production capacity, highlighting the vulnerability of modern, interconnected supply chains.



Recent research indicates that:

- The average ripple event impacts 10 firms beyond the original victim.
- The largest ripple event touched 131 firms downstream.
- Ripple events are growing more common, increasing on average by 20% annually.
- Supply chain disruptions lasting just 30 days or less can jeopardize 3-5% of a company's EBITDA margin.

04

The Era Of Automation: Opportunities And Challenges

A. Benefits of automation in business processes

Automation has become a cornerstone of modern business operations, offering numerous advantages across various functions:

1. Increased Efficiency

Automated processes can operate 24/7 without fatigue, significantly increasing productivity and reducing cycle times.

2. Cost Reduction

By minimizing manual interventions, automation can lead to substantial cost savings in labor and operations.

3. Improved Accuracy

Automated systems reduce human error, ensuring consistent quality and precision in repetitive tasks.

4. Scalability

Automation enables businesses to handle increased workloads and expand operations without proportional increases in resources.

5. Data-driven Insights

Automated systems can collect, process, and analyze vast amounts of data, providing valuable insights for decision-making.

6. Enhanced Customer Experience

Automation in customer service, such as chatbots and self-service portals, can improve response times and availability.

7. Compliance And Auditability

Automated processes can enforce consistent adherence to policies and regulations, creating clear audit trails.

8. Faster Time-to-market

By streamlining development and production processes, automation can accelerate product launches and updates.

9. Improved Employee Satisfaction

Automation of routine tasks allows employees to focus on more strategic, creative, and fulfilling work.

10. Competitive Advantage

Organizations leveraging automation effectively can gain a significant edge in operational efficiency and innovation.

B. Digital Trust: Revolutionizing Cybersecurity Through AI

Digital trust is the confidence individuals and organizations place in the reliability, security, and integrity of data, systems, and digital interactions. The emergence of more advanced technologies through digitized home security systems, self-driving cars, sensors, and more causes concern for the digital protection of all assets and not just online data.

I. Components of Digital Trust

01

Security

Digital Trust ensures that digital systems and data are protected from cyber attacks, unauthorized access, data breaches, or any other type of cyber threat. Cybersecurity covers the security of digital assets, except with Digital Trust, it has expanded to everything in the digital interface.

02

Reliability

Another aspect of Digital Trust is making sure that the consumer TRUSTS the software. To achieve this, the consumer needs to know just how reliable the solution is. Through Digital Trust, respecting and protecting individuals' personal data, ensuring that the data and asset information are collected and stored properly, and utilizing the digital architecture without unexpected failures or errors become a lot easier and more efficient. Digital Trust brings an enhanced sense of reliability.

05

Ethical Behavior

Digital Trust is heavily focused on following current cybersecurity standards and policies the right way. By upholding principles of fairness, accountability, and responsibility in the use of digital technologies, Digital Trust promotes an overall safer and standardized method of demonstrating security.

03

Transparency

One component of Digital Trust that consumers emphasize is transparency. A Digital Trust platform provides clear and understandable information about how data is collected, used, and shared. Through this approach, various companies, homes, and businesses can determine exactly what is happening with their network and how everything operates so they can take the safest and most beneficial steps toward digital safety.

04

Privacy

One major part of excelling in the security, reliability, and transparency facets of digital trust is making sure everything is private. Privacy in Digital Trust refers to keeping individuals' data private and ensuring that it is collected, stored, and used transparently and securely where only the consumer can edit or view their software and network reports.

II. AI on the Rise with Cyber

As AI continues to evolve and integrate into daily life, the realization dawns that its influence transcends mere convenience; it has become indispensable, shaping how we work, communicate, and even make decisions, fundamentally altering the way we live. Artificial intelligence has significantly transformed the landscape of cybersecurity, presenting both valuable opportunities and meticulous challenges.

AI's capacity for rapid data analysis, pattern recognition, and predictive modeling has enabled more robust and proactive defense mechanisms against cyber threats. Machine learning algorithms can more efficiently detect anomalies and potential security breaches, often in real-time, allowing organizations to respond more effectively to attacks.

AI-driven systems can also adapt to evolving threats, learning from each incident to enhance future security measures

C. Increased reliance on third-party services and technologies

The adoption of automation has coincided with and often necessitated an increased reliance on third-party services and technologies:



Cloud-Based Services & Platforms

- SaaS platforms
- Data analytics platforms
- AI and ML services



Cybersecurity & Risk Management

- Managed security services



Financial & Transaction Services

- Payment processing



Automation & IoT

- RPA tools and networks
- IoT devices
- Supply chain automation

D. New risk vectors introduced by automation

While automation offers significant benefits, it also introduces new cybersecurity challenges and risk vectors:

1. Expanded attack surface

The integration of multiple automated systems and third-party services increases the number of potential entry points for attackers.

2. Complexity and visibility challenges

The intricate web of automated processes and integrations can make it difficult to maintain visibility and control over all system components.

3. Rapid propagation of errors

Automated systems can quickly amplify and spread the impact of errors or malicious actions across interconnected processes.

4. Overreliance on automation

Excessive dependence on automated systems without adequate human oversight can lead to blind spots in risk management.

5. Data privacy concerns

Automated data collection and processing can raise privacy issues, especially when involving third-party services.

6. API vulnerabilities

The increased use of APIs in automated processes introduces potential security weaknesses if not properly secured.

7. Credential abuse

Automated systems often require privileged access to various resources, making them attractive targets for credential theft and abuse.

8. Scalable attack vectors

Attackers can leverage automation to scale their malicious activities, such as automated scanning for vulnerabilities or credential stuffing attacks.

9. Supply chain vulnerabilities

Automation in supply chains can create new avenues for supply chain attacks and disruptions.

10. Compliance challenges

The complex interplay of automated processes and third-party services can complicate regulatory compliance efforts.

As organizations navigate this landscape of opportunities and challenges, it becomes increasingly clear that traditional approaches to third-party risk management are no longer sufficient. In the following sections, we'll explore how automation can be leveraged not just as a source of risk, but as a powerful tool for managing and mitigating third-party cyber exposures in this new era.

D. Bringing It All Together: Security Risks At The Intersection Of IOT And Automation In The Supply Chain

As supply chains become more interconnected, the convergence of Automation, IoT (Internet of Things), and Supply Chain operations is reshaping industries. While these technologies improve efficiency, they also introduce new cybersecurity risks that attackers can exploit.

IoT and Automation drive supply chain innovation in various ways today:

1 IoT Sensors & Smart Devices

Enable real-time tracking of goods, predictive maintenance, and inventory management.

2 RPA & AI-Driven Automation

Automate repetitive tasks, optimize logistics, and enhance decision-making.

3 Smart Manufacturing & Warehousing

IoT-driven automation systems reduce downtime and improve efficiency.

However, this comes with some significant security risks, including:

1 Unsecured IoT Devices

Weak authentication and outdated firmware create attack entry points.

2 Automated Cyber Threat Propagation

Compromised IoT devices and RPA tools can be used to spread malware across networks.

3 Supply Chain Dependencies

Attackers exploit third-party automation platforms to gain access to broader ecosystems.

05

Current Approaches To Third-Party Risk Management

A. Traditional manual assessment methods

Historically, organizations have relied on various manual methods to assess and manage third-party risks:

- 1 Questionnaires and surveys:** Send detailed security questionnaires to vendors to gather information about their security practices and controls.
- 2 On-site audits:** Conduct physical inspections of vendor facilities and systems to verify security measures.
- 3 Document reviews:** Examine vendor policies, procedures, and compliance certifications.
- 4 Point-in-time assessments:** Perform periodic security assessments or penetration tests on vendor systems.
- 5 Contract reviews:** Analyze vendor contracts for security and compliance clauses.
- 6 Financial health checks:** Assess the financial stability of vendors to gauge operational risk.
- 7 Background checks:** Conduct due diligence on vendor ownership and key personnel.

- 8 **Reference checks:** Contact other clients or industry peers for feedback on vendor performance and reliability.
- 9 **Manual risk scoring:** Assign risk scores to vendors based on collected information and subjective assessments.
- 10 **Periodic reassessments:** Repeat the assessment process at regular intervals, often annually.

B. Limitations of manual approaches in the digital age

While these traditional methods have served organizations well in the past, they face significant limitations in today's rapidly evolving digital landscape:

1. **Time and resource intensity:** Manual assessments are labor-intensive and time-consuming, limiting the frequency and scope of evaluations.
2. **Scalability issues:** As the number of third-party relationships grows, manual processes become increasingly unsustainable.
3. **Point-in-time nature:** Traditional assessments provide only a snapshot of vendor risk, failing to capture the dynamic nature of cyber threats.
4. **Subjectivity and inconsistency:** Manual assessments often involve subjective judgments, leading to inconsistencies across evaluations.
5. **Limited visibility:** Questionnaires and periodic audits may not provide a complete picture of a vendor's actual security posture.

6. **Delayed response to changes:** Manual processes are slow to detect and respond to changes in vendor risk profiles or security incidents.
7. **Data accuracy and currency:** Information collected through manual processes can quickly become outdated in rapidly changing environments.
8. **Difficulty in prioritization:** Manual methods often struggle to effectively priority.

C. The need for a paradigm shift

The limitations of traditional manual approaches, combined with the increasing complexity and dynamism of the digital business environment, necessitate a fundamental shift in how organizations approach third-party risk management:

1. **From periodic to continuous:** The rapid pace of technological change and the evolving threat landscape demand a shift from point-in-time assessments to continuous monitoring and evaluation of third-party risks.
2. **From reactive to proactive:** Organizations need to move beyond responding to incidents after they occur and adopt proactive strategies that anticipate and mitigate potential risks before they materialize.
3. **From manual to automated:** To address scalability issues and improve efficiency, there's a critical need to automate key aspects of the risk management process.
4. **From siloed to integrated:** Third-party risk management must be integrated with broader enterprise risk management and cybersecurity frameworks for a holistic approach.
5. **From static to dynamic:** Risk assessments need to evolve from static, checklist-based approaches to dynamic, context-aware evaluations that adapt to changing conditions.

6. **From limited to comprehensive:** Risk management strategies must expand beyond immediate vendors to encompass the entire ecosystem of third, fourth, and nth-party relationships.
7. **From compliance-focused to risk-focused:** While maintaining compliance is crucial, organizations need to prioritize a risk-based approach that goes beyond mere checkbox exercises.
8. **From human-centric to AI-augmented:** Leveraging artificial intelligence and machine learning can enhance human decision-making and automate complex risk analyses.
9. **From retrospective to predictive:** Advanced analytics and threat intelligence should be employed to forecast potential risks and vulnerabilities.
10. **From subjective to data-driven with Digital Trust Scoring:** Vendor criticality is a key quantifiable factor in assessing and managing digital trust while digital trust scores provide a quantifiable measure of the vendor's trustworthiness. Upon integration with a robust vendor onboarding process, you can leverage Digital Trust scores as a tool to provide a structured assessment of trust.

Digital Trust Scores

RANGE	RATING
300-579	Poor
580-669	Fair
670-739	Good
740-799	Very Good
800-850	Excellent

This paradigm shift is essential for organizations to effectively manage third-party cyber risk exposures in the era of automation. By embracing new technologies and approaches, businesses can transform their risk management capabilities to match the speed and complexity of the modern digital ecosystem.



Leveraging Automation For Third-Party Cyber Risk Management



Continuous monitoring and real-time risk assessment

Automation enables organizations to move beyond periodic assessments to continuous, real-time monitoring of third-party risks:

1. **Network monitoring:** Automated tools can continuously scan third-party network connections for potential vulnerabilities or suspicious activities.
2. **Threat intelligence integration:** Automated systems can incorporate real-time threat intelligence feeds to identify emerging risks associated with third parties.
3. **Continuous compliance checking:** Automated tools can continuously verify third-party compliance with relevant standards and regulations.
4. **Real-time alerting:** Automated systems can generate instant alerts when significant changes in a vendor's risk profile are detected.



Automated due diligence and vendor onboarding

Automation can streamline and enhance the vendor onboarding and due diligence process:

1. **Tiered questionnaires:** Intelligent systems can generate tailored questionnaires based on vendor profiles and automatically validate responses.

2. **Document analysis:** AI-powered tools can quickly analyze vendor documentation for relevant security and compliance information.
3. **Digital footprint analysis:** Automated systems can scan public and dark web sources to gather intelligence on potential vendors.
4. **Background checks:** Integration with various databases can facilitate rapid background checks on vendor organizations and key personnel.
5. **Contract analysis:** Natural Language Processing (NLP) can be used to automatically review and flag potential issues in vendor contracts.

AI-driven predictive risk analytics

Advanced AI and machine learning techniques can provide predictive insights into third-party risks:

1. **Risk trend analysis:** AI models can analyze historical data to identify trends and predict future risk levels for individual vendors or categories.
2. **Scenario modeling:** Automated systems can simulate various risk scenarios to help organizations prepare for potential third-party incidents.
3. **Vulnerability prediction:** Machine learning algorithms can predict potential vulnerabilities in third-party systems based on various data points.
4. **Impact assessment:** Automated tools can model the potential impact of third-party incidents on various aspects of the business.

Automated policy enforcement and compliance checking

Automation can ensure consistent application of security policies and compliance requirements:

1. **Access control:** Systems can automatically grant, modify, or revoke third-party access based on predefined policies and real-time risk assessments.
2. **Compliance monitoring:** Automated tools can continuously check third-party systems and practices against relevant compliance standards.
3. **Policy violation alerts:** Automated systems can instantly flag and alert on any deviations from established security policies.
4. **Remediation:** Some issues can be automatically remediated based on predefined rules and workflows.
5. **Audit trail generation:** Automated systems can maintain comprehensive logs of all third-party interactions and policy enforcement actions.

By leveraging these automated approaches, organizations can significantly enhance their ability to manage third-party cyber risk exposures effectively.

This shift towards automation not only improves the scalability and efficiency of risk management processes but also enables a more proactive and dynamic approach to addressing the complex challenges of the modern digital ecosystem.

07

Key Components To Look Out For In An Automated Third-party Risk Management Program

A. Asset discovery and inventory management

An effective automated third-party risk management program begins with a comprehensive understanding of all third-party relationships and assets:

1. **Automated asset discovery:** Utilize network scanning and API integrations to automatically identify and catalog all third-party connections and assets.
2. **Dynamic inventory updates:** Implement systems that automatically update the third-party asset inventory as new connections are established or removed.
3. **Classification and categorization:** Use AI-driven tools to automatically classify third-party assets based on criticality, data sensitivity, and potential impact.
4. **Relationship mapping:** Employ graph database technologies to map complex relationships between various third, fourth, and nth parties.
5. **Integration with existing systems:** Ensure the asset discovery and inventory management system integrates seamlessly with existing IT asset management and procurement systems.

B. Vulnerability scanning and threat intelligence integration

Automated vulnerability management and threat intelligence are crucial for maintaining an up-to-date risk profile:

1. **Continuous vulnerability scanning:** Implement automated scanners that regularly check third-party systems for known vulnerabilities.
2. **Threat intelligence feeds:** Integrate real-time threat intelligence feeds to stay informed about emerging threats and vulnerabilities affecting third parties.
3. **Automated patch verification:** Use automated tools to verify that third parties are applying critical security patches on time.
4. **Dark web monitoring:** Employ automated dark web scanning to detect potential data leaks or cyber threats related to third parties.
5. **Risk contextualization:** Utilize AI to contextualize vulnerabilities and threats based on the specific third-party relationship and potential business impact.

C. Automated risk scoring and prioritization

Develop a dynamic, data-driven approach to assessing and prioritizing third-party risks:

1. Multi-factor risk scoring

Implement an automated risk scoring system that considers various factors such as vulnerabilities, threats, compliance status, and business criticality.

2. Machine learning-based risk models

Utilize machine learning algorithms to continuously refine and improve risk scoring models based on new data and evolving threat landscapes.

3. Automated risk prioritization

Use AI to automatically prioritize risks based on potential impact, likelihood, and organizational risk appetite.

4. Trend analysis and forecasting

Implement predictive analytics to identify risk trends and forecast potential future risks.

5. Customizable risk thresholds

Allow for the setting of automated alerts based on customizable risk thresholds for different types of third-party relationships.

D. Workflow automation for risk mitigation and incident response

Streamline and accelerate risk mitigation and incident response processes through automation:

1. Automated remediation workflows

Develop automated workflows that trigger specific remediation actions based on identified risks or policy violations.

2. Escalation and notifications systems

Implement automated escalation procedures and notification systems to ensure timely response to high-priority risks.

3. Incident Response Playbooks

Create automated incident response playbooks that guide teams through predefined steps in case of a third-party security incident.

4. Automated Reporting

Generate automated risk reports and dashboards to keep stakeholders informed of the current third-party risk landscape.

5. Task Management and Tracking

Utilize workflow automation tools to assign, track, and manage risk mitigation tasks across the organization.



Integration with existing security and GRC platforms

Ensure that the automated third-party risk management system integrates seamlessly with other key organizational systems:

1. **SIEM integration:** Connect the third-party risk management system with Security Information and Event Management (SIEM) platforms for comprehensive threat detection and response. Integrating Third-Party Risk Management (TPRM) with SIEM platforms enhances threat detection by centralizing vendor-related security events. This enables real-time monitoring, anomaly detection, and automated alerts, ensuring faster incident response. AI-driven analysis improves risk visibility, strengthens compliance, and reduces supply chain vulnerabilities for a more resilient cybersecurity posture.
2. **GRC platform connectivity:** Integrate with Governance, Risk, and Compliance (GRC) platforms to ensure alignment with overall risk management and compliance efforts.
3. **Identity and Access Management (IAM) integration:** Connect with IAM systems to automate the management of third-party access rights based on risk assessments.
4. **API-driven integrations:** Develop robust API connections to enable seamless data flow between various security and risk management tools.
5. **Data analytics platform integration:** Connect with data analytics platforms to enable advanced risk analytics and reporting capabilities.

By implementing these key components, organizations can create a comprehensive, automated third-party risk management program that is both efficient and effective in addressing the complex challenges of modern cyber risk exposures.

08

Implementing An Automated Third-Party Risk Management Strategy

A. Assessing organizational readiness

Before embarking on the implementation of an automated third-party risk management strategy, it's crucial to assess the organization's readiness:

1. **Current state analysis:** Evaluate existing third-party risk management processes, identifying gaps and areas for improvement.
2. **Stakeholder alignment:** Ensure buy-in from key stakeholders across the organization, including IT, security, procurement, and legal teams.
3. **Resource assessment:** Determine the availability of necessary resources, including budget, personnel, and technological infrastructure.
4. **Data quality evaluation:** Assess the quality and completeness of existing third-party data, as this will be crucial for effective automation.
5. **Regulatory compliance review:** Understand the regulatory requirements that may impact the implementation of automated risk management processes.

B. Selecting the right tools and technologies

Choosing the appropriate tools and technologies is critical for successful implementation:

1. **Vendor evaluation:** Conduct a thorough evaluation of potential vendors offering automated third-party risk management solutions.
2. **Scalability and flexibility:** Ensure that chosen solutions can scale with the organization's needs and adapt to changing risk landscapes.
3. **Integration capabilities:** Prioritize tools that offer robust integration capabilities with existing systems and data sources.

4. **AI and machine learning capabilities:** Look for solutions that leverage advanced AI and machine learning for predictive analytics and decision support.
5. **Customization options:** Select tools that allow for customization to meet the organization's specific risk management needs and processes.

C. Training and change management considerations

Effective implementation requires a focus on people and processes, not just technology:

1. **Stakeholder education:** Provide comprehensive training to all stakeholders on the new automated risk management processes and tools.
2. **Role and responsibility definition:** Clearly define roles and responsibilities within the new automated risk management framework.
3. **Cultural shift:** Foster a culture of continuous risk awareness and management across the organization.
4. **Change management strategy:** Develop a comprehensive change management plan to address potential resistance and ensure smooth adoption.
5. **Ongoing support and training:** Establish mechanisms for ongoing support and training as the automated system evolves and expands.

By carefully considering these implementation factors, organizations can maximize the chances of successfully transitioning to an automated third-party risk management strategy. This approach will enable them to more effectively address the complex cyber risk exposures in today's rapidly evolving digital landscape.



Best Practices For Third-Party Risk Management

Effective third-party risk management has become a critical component of organizational success. As you rely on external partners, vendors, and service providers for everyday business processes, ensure to implement these robust strategies to protect your operations, reputation, and financial health.

- 🔑 Staff third-party risk management teams with qualified, experienced professionals to ensure effective oversight and risk mitigation.
- 🔑 Continuously monitor industry developments and regulatory enforcement actions to maintain an up-to-date risk management strategy. As the saying goes, “You can't fight to win an enemy you don't know”.
- 🔑 Prioritize vendor criticality as part of a robust vendor onboarding program.
- 🔑 Establish and maintain comprehensive, up-to-date governance documents, including policies, standards, programs, and procedures.
- 🔑 Regularly update assessments, questionnaires, and due diligence requirements to reflect the evolving risk landscape.
- 🔑 Educate vendor owners and management about third-party risk management objectives, and provide training to help them fulfill their responsibilities effectively.
- 🔑 Evaluate the effectiveness of third-party risk management using quantifiable metrics and comprehensive program assessments.
- 🔑 Systematically document, monitor, and address vendor issues until full resolution.

- 🔑 Cultivate a culture of continuous improvement.
- 🔑 Monitor vendor Digital Trust Scores and External Risk Views as part of vendor relationship lifecycle management.
- 🔑 Provide regular, comprehensive updates to executive leadership and the board of directors.

Our Recommendation

Follow a holistic approach, beginning with thorough vendor vetting and extending through continuous monitoring and incident response planning.

By embracing comprehensive risk assessments, establishing clear contractual agreements, and maintaining strong internal controls to build resilient relationships with third-party ecosystems.

Also, a tiered, risk-based approach allows you to allocate resources efficiently, focusing more attention on high-risk partners while maintaining appropriate oversight across all relationships.

Baumgartner, T., Malik, Y., & Padhi, A. (2020, August 11). Reimagining industrial supply chains. McKinsey & Company. <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/reimagining-industrial-supply-chains>

Kissflow. (2025, February 27). 20+ key business process Automation stats You need to know. <https://kissflow.com/workflow/bpm/business-process-automation-statistics/#:~:text=Companies%20that%20successfully%20integrate%20AI,businesses%20will%20continue%20to%20increase>

McCann, K. (2024, November 12). Amazon: How MOVEit Supply Chain Attack Left Echoing Effects. Cyber Magazine. Retrieved January 9, 2025, from <https://cybermagazine.com/articles/amazon-how-moveit-supply-chain-attack-left-lasting-effects>

Mittal, M. (2024, December 30). Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience. Research Gate. Retrieved February 5, 2025, from https://www.researchgate.net/publication/387779329_Colonial_Pipeline_Cyberattack_Drives_Urgent_Reforms_in_Cybersecurity_and_Critical_Infrastructure_Resilience

The Total Economic Impact™ of BMC Helix - BMC Software. (n.d.). BMC Software. <https://www.bmc.com/forms/forrester-report-total-economic-impact-of-bmc-helix-itconcepts.html>

Whittaker, Z. (2025, January 24). UnitedHealth confirms 190 million Americans affected by Change Healthcare data breach. TechCrunch. <https://techcrunch.com/2025/01/24/unitedhealth-confirms-190-million-americans-affected-by-change-healthcare-data-breach/>

WorkMarket. (2020). 2020 In(Sight): What AI & Automation really mean for work. [https://images.adpinfo.com/Web/ADPEmployerServices/%7B085dfeb6-e471-4e88-b8fb-dc0b2b9b2b07%7D_2020-In\(Sight\)-Report.pdf](https://images.adpinfo.com/Web/ADPEmployerServices/%7B085dfeb6-e471-4e88-b8fb-dc0b2b9b2b07%7D_2020-In(Sight)-Report.pdf)

Next Steps

Download your free copy

Explore the latest updates with our reports. Download your free copy now to stay abreast with industry trends.



Download Here



Download Here

About DigitalXForce

DigitalXForce, "Digital Trust for the New Era," is an AI-Powered Enterprise Security Risk Posture Management (ESRPM) and GRC SaaS Platform enabling Real-time, Continuous, and Automated Third-Party Risk Management through Cybersecurity Mesh Architecture with data-driven insights, security blueprints, and regulatory control mapping.

Existing Integrated Risk Management (IRM) and Governance Risk Compliance (GRC) platforms fail the ultimate cybersecurity mission of securing digital assets by focusing solely on audit and compliance using outdated artifacts, neglecting active security posture management. Qualitative cyber risk evaluation lacks scalability and relevance, leaving compliant companies vulnerable to breaches.

DigitalXForce tackles the "Compliance $\neq$ Security" problem. The Digital Trust platform's unique approach combines AI/ML techniques, direct security tool integration, and comprehensive asset management to provide a more accurate, efficient, and actionable risk management solution compared to traditional GRC platforms.

DigitalXForce develops all functions in-house, including crucial security connectors, using proprietary toolkits. The company's proprietary AI model, dubbed XForce GPT, enables continuous learning and improvement of compliance control mappings for risk quantification.

Additional Resources

[Our Solutions](#)

[Request a Demo](#)

[Frameworks](#)

[Industries](#)

[Announcements](#)

[Whitepapers](#)

[Articles](#)

[Events](#)

[Awards](#)

Connect With Us



