INFOSEC WORLD

2023 TRENDS REPORT

TODAY'S RISKS TOMORROW'S THREATS

RISK, RESILIENCE, AND RESPONSE

INFOSEC WORLD
SEPT 25-27, 2023

infosecworldusa.com

INFOSEC WORLD 2023: 5 TRENDS

InfoSec World celebrates its 29th anniversary this year, and much has changed since MIS Training Institute introduced the conference in 1994. Back then, security practitioners were concerned about the increasing connectivity of machines and organizations, the lack of end-user awareness and senior management support, budget constraints and technical complexities. We're still wrestling with many of those issues today, but as the world has become interconnected, other issues have come to light.

Security teams must now deal with a multitude of cloud security concerns, ongoing governance and compliance issues on the local, national and international level, the ever-present threat of cybercrime and fraud, privacy concerns and now the introduction of AI solutions and threats.

Staying ahead of these threats and gaining the latest insight from other practitioners and organizations is the focus of the InfoSec World conference program. We're thrilled to be able to bring industry leaders together to discuss, debate, learn and connect this September in Orlando, Florida. The annual InfoSec World conference call for presentations provides a unique window into how the cybersecurity and information security functions within organizations are responding to the shifting demands for business growth and regulatory compliance.

This year we're delighted to release the first annual InfoSec World Trends Report, informed by a review of hundreds of call-for-presentation responses, refined by discussions with members of the InfoSec World Advisory Board and other industry luminaries, and put into context with survey research and other content produced by CyberRisk Alliance.

This report examines five trends that surfaced from the pool of submitted presentations and recent news events, providing insight into the priorities of leaders, executives, and digital identity professionals to inform your cybersecurity strategy for the next 12-18 months.

TO LEARN MORE:

Visit the InfoSec World Website ›

Attend the InfoSec World Conference ›

KEY TRENDS:

TREND 1

The Emergence of Artificial Intelligence Tools and Threats

AI concerns have exploded in the last six months, particularly with the introduction of ChatGPT. Users are seeking facts - not FUD - about the topic and are concerned about how they can leverage this technology for improved security, and how to defend against it as threat actors take advantage of the technology.

Rohit Ghai, CEO of RSA Security, recently predicted that AI will continue to fuel further disruption with cybersecurity products and services and that "many jobs will disappear, many will change, and some will be created." Of course, AI could benefit organizations as it takes on and automates such tasks as investigating false positives and helping to augment what humans can do.

Meanwhile, threat actors are leveraging AI to carry out their crimes - generating phishing emails, malicious code or using chatbots to carry on messaging conversations with the aim of getting the target to send PII (like SSN) or funds to them. These attacks and fraud schemes are increasing in sophistication, frequency, and speed.

With the introduction of open-source generative AI tools, a quickly emerging field is that of AI Governance. Certain countries and municipalities have released their own frameworks on governance and ethics. Organizations like IAPP have established AI Governance centers to provide content, resources, networking, training and certification needed for this emerging area.

InfoSec World 2023 will offer sessions ranging from "Handling Risks for AI Coding Assistants", "Misinformation in the Age of Generative AI", "Some Legal Perspectives on ChatGPT and What it Means for Your Infosec Program" to "Should I Trust ChatGPT to Review My Program?".

TREND 2

The Increase of Governance, Compliance, and Regulatory Acts

Organizations are focused on Governance, Risk, and Compliance (GRC) issues as more states and countries introduce different laws and regulations aimed at cybersecurity. These range from breach notification guidance, a new version of PCI DSS set to make its debut, pending Securities and Exchange Commission (SEC) regulations and the emergence of governance of AI usage.

The SEC proposes to require the disclosure of "material" cybersecurity incidents within four business days to the Cybersecurity & Infrastructure Security Agency (CISA) and investors (disclosure would be required after a company determines that a cybersecurity incident was material). However, the definition of "materiality" is in question. Additionally, the SEC also wants companies to anticipate and mitigate cyber risk. InfoSec World will offer a session focused on this topic: Time After Time': Preparing for the SEC's New Timeline for Incident Reporting.

The Payment Card Industry Data Security Standard (PCI DSS) v4.0 goes into effect on March 31, 2024 and includes more than 60 new requirements for organizations that take payment cards. Organizations need to start preparing for the updated standard and develop a road map for the changes to the people-process-technology triad that PCI DSS v4.0 will bring. InfoSec World will present two sessions focused on this important topic: Confessions of a QSA: Navigating PCI DSS 4.0 and How to Harness the IT Security Powers of the new PCI-DSS v4.0.

There's no doubt that CISOs and other security leaders are in the crosshairs. In October 2022, Uber CISO Joe Sullivan was convicted in federal court of charges stemming from his actions in response to a 2016 breach of Uber. It was an unprecedented decision and has brought to the surface many concerning questions for CISOs who now feel they are squarely in an unwanted law enforcement spotlight.

It's incumbent upon CISOs and security leaders to work together with their legal counsel(s) for better understanding of legal, compliance and governance issues. InfoSec World will cover this topic in two different sessions: Benefits of Legal and CISOs Uniting in a Post-Uber and Twitter World and The Uber CISO Prosecution and What it Means for Your Infosec Program.

The complex threat landscape is impacting these new standards and compliance acts. Insecure software is playing a role in bad actors gaining a foothold and access to corporate systems. The current administration has taken the position that opening up companies to potential lawsuits tied to poorly developed software, while creating a legal safe harbor for those that follow best practices, could move the industry to "secure by design software development" and away from pointing the blame a end users when a system is breached.

Kelly Shortridge, a senior principal at Fastly, told SC Media "How do you deem what is negligent or not? Is it just someone who is very bad, and they actually didn't care about security? Especially smaller businesses [where] it's a trade-off between 'Do I move quickly and compete in the market?' or 'Do I invest a lot in security?' That's just not a healthy trade-off."

Chris Romeo, CEO of Kerr Ventures, will examine "The Application Security State of the Union" with a session at InfoSec World in which he examine areas of innovation and the items needed for success in future years.

The Emergence of AI Tools and Threats

The Ongoing Complexity of Securing the Cloud

The Ever-Expanding Threat Landscape

The Increase in Governance, Compliance and Regulatory Acts

A Workforce that Continues to be Stretched Thin and Under Constant Stress

The Ongoing Complexity of Securing the Cloud

Most organizations have rapidly accelerated their cloud migration in response to the pandemic and emergence of the hybrid workforce that has followed it. In fact, Flexera says 94% of enterprises use the cloud while 62% are looking at optimizing the existing use of their cloud.

Misconfiguration of the cloud is a big concern for organizations. Issues can range from a failure to change default setting, allowing overly permissive access, the lack of strict monitoring and logging, as well as neglecting third-party components. These misconfigurations can lead to data leakage and breaches. Proofpoint reported that 2021 data from their customer base showed more than 90% of monitored cloud tenants were targeted each month, with 24% successfully attacked.

These data breaches bring negative publicity and organizations are starting to be held responsible and fined if it's found that the breach was the result of failing to secure their cloud environment. In June of 2022, the grocery chain Wegmans was fined $400,000 by the New York State Attorney General for allegedly exposing PII of 3 million customers.

In 2023, Meta was fined by the Irish Data Protection Commission under GDPR for €1.2 billion when it was found that the company did not have the appropriate technical and organizational measures in place to readily demonstrate implemented security measures being used to protect EU users' data in the context of breaches and were unlawfully transferring European user' data to its US-based servers and taking no suuicient measures to ensure users' privacy.

As the cloud environment grows at organizations, challenges in managing and defending against cyberattacks, an increasing regulatory environment, gaining greater visibility and reining in tool sprawl continue to be a concern. Security teams are focused on designing effective security controls and leveraging the features in the cloud platform(s) they are using. InfoSec World will hold a session that focuses on securing Azure applications, a full day Cloud Security summit and a two-day Masterclass on securing AWS and Azure infrastructures.

The Emergence of AI Tools and Threats

The Ongoing Complexity of Securing the Cloud

The Ever-Expanding Threat Landscape

The Increase in Governance, Compliance and Regulatory Acts

A Workforce that Continues to be Stretched Thin and Under Constant Stress

TREND 4

A Workforce That Continues to Be Stretched Thin and Under Constant Stress

They say it "starts at the top." For security departments, that's with the CISO. However, the 2022 Global Chief Information Security Officer (CISO) survey reported stress (54%), burnout (35%) and a competitive hiring market is leading to higher than usual turnover (34%). It's no wonder they are facing these pressures.

Organizations cannot find enough qualified professionals to fill the roles in their security departments. The competition for experienced practitioners is fierce and organizations are paying top-dollar to fill these openings. The existing security staff needs to be resilient in the face of having to do more with less, continuous threats and a stressful job. The talent pipeline is somewhat bare and finding and retaining cybersecurity talent is at the forefront of concerns for most organizations.

Forbes reported that there are approximately 4.7 million professionals in the cybersecurity workforce, but there's still a major shortfall. In their 2022 Cybersecurity Workforce Study, ISC² reported a worldwide gap of 3.4 million cyber-security workers. This shortage impacts organizations' ability to achieve compliance and secure their data. The technology and the threats morph very quickly, and practitioners struggle to keep pace. This results in fatigue, stress, and burnout.

Companies continue to try and train and retain their own staff, but the competition for experienced cybersecurity professionals is fierce. This is one of the top challenges for the public sector. SC Media reports that in 2023, the inability to hire and retain appropriately trained and experienced talent to defend against the high volume of attacks will leave the public sector highly vulnerable. Marcin Kleczynski, CEO of Malwarebytes, predicts that a nationally significant attack directly attributed to an under-resourced security team will be a breaking point.

Many organizations are focusing on diversity. AI will play a role in helping with the workforce shortage, as automation takes over some mundane tasks (such as false positives), however, many organizations are looking for real human individuals with diverse backgrounds and talents. Diversity can no longer be a "check-the-box" exercise. Barriers are starting to be broken and this momentum will need to continue.

InfoSec World will focus on the workforce shortage, burnout and need for diversity with several sessions including the Need for Cybersecurity apprenticeships, Beyond Burnout: Where We Are Today and What We Need To Do Now, Stress Management for Security and Women in Cybersecurity (Powering up the Cybersecurity Workforce by Keeping an Eye on the "I".

The Emergence of AI Tools and Threats

The Ongoing Complexity of Securing the Cloud

The Ever-Expanding Threat Landscape

The Increase in Governance, Compliance and Regulatory Acts

A Workforce that Continues to be Stretched Thin and Under Constant Stress

The Ever-Expanding Threat Landscape

Meanwhile, for security teams of all sizes and industries, threats continue to multiply. Organized crime and nation/state attacks are only the tip of the threat iceberg. Threats like phishing and BEC leading to fraud and ransomware require continual monitoring. Insiders, whether their actions are malicious or accidental are always a concern.

AI is rapidly improving the capabilities of both defenders and attackers. Adversarial AI is expanding the attack surface and being used two ways: attacks that use AI and attacks against AI. Deepfakes and BEC operations are examples of attacks leveraging AI while gaining access and "poisoning" the data decision library in an AI system (so the wrong information is output is an example of a target attack against an AI system. Threat modeling and threat detection are taking these new, emerging threats into account. However, sharing of information on these new attacks needs to improve to help the cybersecurity community remain safe and secure.

InfoSec World will hold a session on this topic (Machine Readable Representations of Cyber Adversary Behavior with STIX) lead by a representative from Johns Hopkins Applied Physics Laboratory.

It's been said that just because you can threat hunt doesn't mean you should threat hunt. Many organizations simply don't have the training or infrastructure to effectively operate and manage a threat hunting program that provides tangible benefits. A solid foundation needs to be in place.

InfoSec World will provide useful information on threat hunting in two workshops. Cloud Native Application Architecture Threat Hunting will help attendees to build and refine knowledge, skills and capabilities to hunt for threats against enterprise cloud deployments).

The two-day Adversarial Purple Teaming workshop will examine the "purple team" approach as it goes through tactics, techniques and procedures (TTPs) of attacks while building knowledge on how to write rules that focus on behavior exhibited in order to better detect and defend).

The recent Verizon Data Breach Investigation Report (DBIR) disclosed that DDoS attacks are getting worse and Ransomware incidents were holding steady (but with room to grow). The most common entry point into a system? Email, desktop applications and web applications. Only a fraction of breaches (5%) reported in the DBIR involved exploiting security vulnerabilities in systems or devices.

To help educate on these vulnerabilities, InfoSec World will hold sessions on "Recipe for Securing Your APIs" and "Does Your DevSecOps Pipeline Only Function as Intended?".

The Emergence of AI Tools and Threats

The Ongoing Complexity of Securing the Cloud

The Ever-Expanding Threat Landscape

The Increase in Governance, Compliance and Regulatory Acts

A Workforce that Continues to be Stretched Thin and Under Constant Stress

INFOSEC WORLD

RISK, RESILIENCE, AND RESPONSE

In Summary

These five trends of course merely scratch the surface of what cybersecurity practitioners need to concern themselves with each day. The InfoSec World conference will cover a myriad of other topics like a Zero Trust Summit, a CISO's Guide to Cultivating Board Support workshop, an Analysis 1010 for Incident Responders workshop, a SOC Fundamentals workshop and a Foundational Zero Trust Network Security workshop.

Other highlights include an Identity Management Summit (powered by the content creators behind Identiverse) and keynotes featuring Rachel Wilson, Managing Director and Head of Cybersecurity, Morgan Stanley Wealth Management and Scott Shapiro, Professor of Law and Philosophy Yale Law School.

The cybersecurity industry moves at lightning speed. Join us September 25th – 27th, 2023 to discover the latest in how to address the challenges security professionals face and to meet and network with follow practitioners!

INFOSEC WORLD
SEPT 25-27, 2023

Disney's Coronado Springs Resort | Lake Buena Vista, Florida

To learn more about InfoSec World, please visit: infosecworldusa.com

Attend the InfoSec World conference ›