Transforming the Business of Information Technology

Richard Ricks
Founder, Managing Partner
& Chief Executive Officer
(CEO)

IT360 Secure

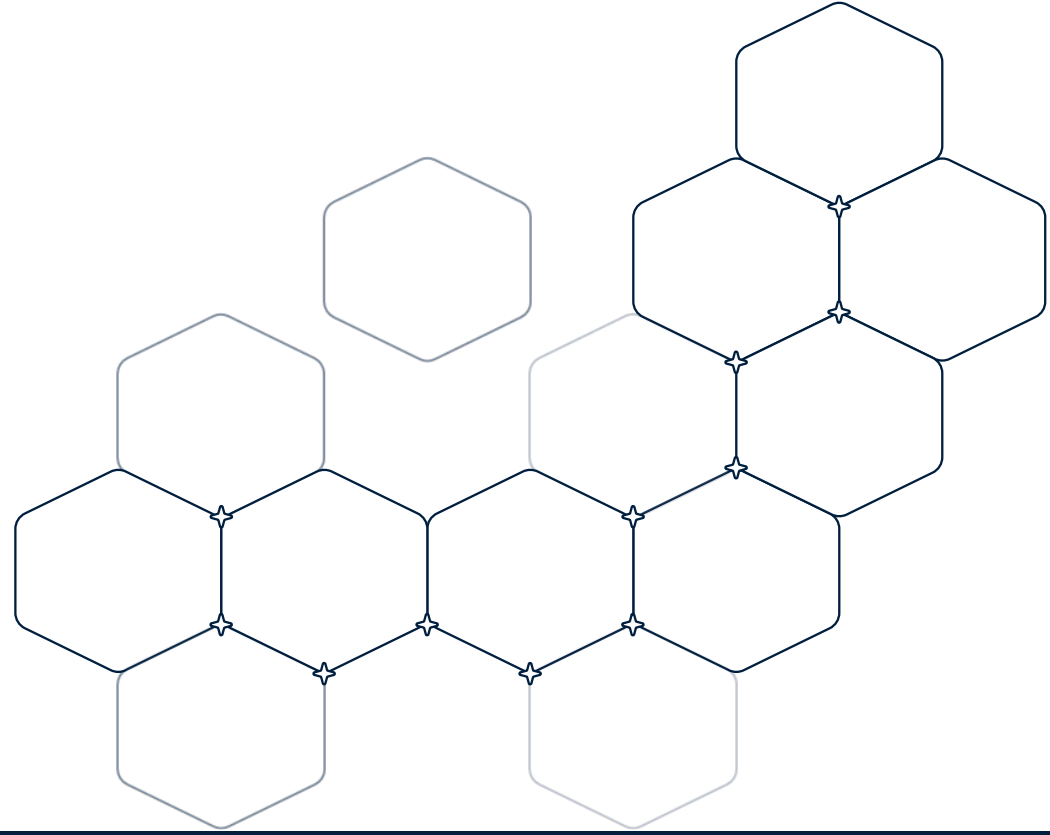
SilverTree

Darwin Herdman
Client Services & Security
Officer (CSSO)

Vigilance™ by SilverTree

servicenow™ HORIZON3.ai TRUST BUT VERIFY Microsoft ScienceLogic

SilverTree



February 14, 2025

State of Cybersecurity Threats in 2025

Cybersecurity in 2025: A constant battle against ever-evolving threats, where vigilance is the only defense

A look back at 2024 – What did we learn?

1

45% of cyber incidents in 2024 were attributed to social engineering attacks, including phishing, pretexting, and impersonation.

2

25% of all cyberattacks were **powered by artificial intelligence** (AI), from automated phishing to AI-driven malware and deepfakes.

3

Over 20 billion records were exposed in data leaks across various sectors in 2024.

4

More than **60%** of small and medium-sized enterprises (SMEs) were **targeted by cyberattacks** in 2024.

What we will see in 2025

Geopolitical Tensions

- State Sponsored Attacks
- Hactivism and Protests
- Supply Chain Vulnerabilities
- Increased Regulatory Pressure

Advanced Persistent Threats

- Quantum Computing-Enabled APTs
- Deeper Integration with AI/ML Tools
- Focus on Cloud & Hybrid Infrastructure
- Biometric Data and IoT-Targeted APTs

Supply Chain Interdependencies

- Third Party Vendor Breaches – Payment Processing, Cloud Storage, accounting and SaaS providers
- Lack of Vendor Management, 3rd Party Risk Assessment or Security Standards

Regulatory Requirements

- Increased Compliance Costs
- Impact on Innovation and Business Agility
- Heightened Risk of Non-Compliance Penalties
- Integration of Privacy & Security Controls

AI Driven Cyber Attacks

- Advanced Deepfake Attacks
- Self Learning Malware and AI enabled Evasion
- Automated Vulnerability Scanning & Exploitation
- AI-Powered Distributed Denial of Service Attacks

Cyber Skills Gap

- Digital Transformation and IT complexity
- Cybersecurity Education & Training Programs
- Burnout and High Turnover Rates
- Global Competition for Cybersecurity Talent

Ransomware as a Service

- Rise in Double and Triple Extortion Models
- Hyper-Personalized & Sophisticated Campaigns
- Increased Attacks from Inexperienced Actors
- Expansion Targeting Critical Infrastructure

Internet of Things Vulnerabilities

- Botnets Powered by IoT Devices
- Privacy Breaches and Data Harvesting
- Device Spoofing and Impersonation
- Weaknesses in IoT Device Integration

Cloud Security Challenges

- Loss of Control Over Data
- Inadequate Cloud Security Configurations
- Insecure APIs and Interfaces

Geopolitical Tensions

State Sponsored Attacks

As nations engage in geopolitical conflicts, they often leverage cyberattacks as part of their broader strategy to disrupt or damage the economies, infrastructure, and institutions of rival states. These attacks are typically more sophisticated, highly coordinated, and persistent, often outpacing the ability of traditional security measures to defend against them.

Hactivism and Protests

These threats often manifest in ways that go beyond traditional cyberattacks and have the potential to disrupt operations, damage reputations, and expose sensitive data. Hacktivists—hackers with political, environmental, or social agendas—may target organizations they perceive as aligned with causes they oppose.

Supply Chain Vulnerabilities

Geopolitical conflicts often lead to increased targeting of critical supply chain partners. In the wake of heightened U.S.-China tensions, Chinese state-sponsored actors have been linked to cyberattacks targeting U.S. companies via vulnerabilities in their software supply chains, such as SolarWinds and Microsoft Exchange

Increased Regulatory Pressure

As conflicts, trade disputes, and international rivalries escalate, governments and regulatory bodies are implementing stricter cybersecurity frameworks and compliance standards to safeguard national interests, protect critical infrastructure, and ensure economic stability.

Advanced Persistent Threats

Quantum Computing-Enabled APTs

With the advent of quantum computing, APT actors will gain access to computational power that can break traditional encryption models (e.g., RSA, AES) much faster than classical computers. This will lead to quantum-enabled attacks on sensitive data, financial systems, and secure communications.

Deeper Integration with AI/ML Tools

Advanced persistent threats will leverage AI for real-time intelligence gathering, pattern recognition, and data exfiltration, outpacing traditional security defenses. AI-driven APTs will be able to change attack vectors dynamically based on the organization's defenses, allowing them to maintain access for extended periods without detection.

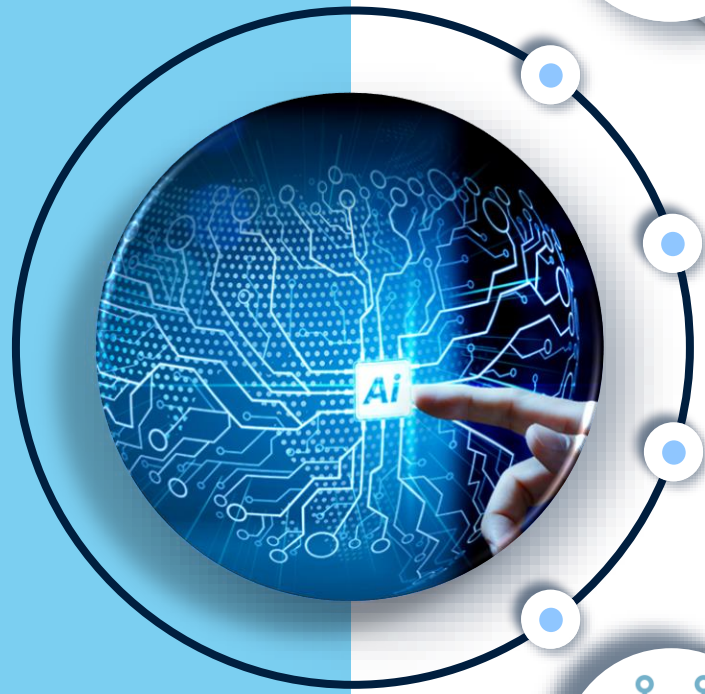
Focus on Cloud & Hybrid Infrastructure

APT actors will target hybrid cloud environments and multi-cloud architectures as organizations continue to transition. Attackers will exploit weak points in cross-cloud security and data governance.

Biometric Data and IoT-Targeted APTs

With the growing reliance on biometric authentication (face recognition, fingerprints, etc.) and IoT devices, attackers will target these technologies as attack vectors. Biometric data manipulation could be used to bypass authentication, and IoT devices could serve as entry points into otherwise secure systems.

AI-Driven Cyber Attacks



Advanced Deepfake Attacks

Deepfake technology will be leveraged in phishing and social engineering attacks at an unprecedented scale. Cybercriminals will use AI to create highly convincing audio and video impersonations of executives, clients, or colleagues, making spear-phishing and business email compromise (BEC) attacks more effective.

AI-Powered DDoS Attacks

Distributed Denial-of-Service (DDoS) attacks will be increasingly powered by AI, making them more targeted and efficient. Attackers will use machine learning algorithms to analyze traffic patterns and adapt the scale and direction of attacks in real time, potentially causing much more severe disruption to critical services

Autonomous Vulnerability Scanning and Exploitation

AI tools will significantly improve the ability of attackers to scan for and exploit zero-day vulnerabilities faster than ever. Machine learning algorithms will allow malicious actors to scan large volumes of code, networks, or systems to detect vulnerabilities autonomously, leading to quicker exploitations before patches are deployed.

Self Learning Malware and AI–Enabled Detection Manipulation

AI-driven malware will become more autonomous and capable of adapting to defenses in real time. AI will help attackers mimic normal network traffic or human behavior, making it extremely difficult for legacy security tools to differentiate between legitimate activity and malicious actions.

Internet of Things Vulnerabilities

Botnets Powered by IoT Devices

IoT devices, such as cameras, routers, smart TVs, and even thermostats, are often poorly secured and are increasingly being hijacked by cybercriminals to form botnets. These botnets can be used to launch large-scale distributed denial-of-service (DDoS) attacks or to carry out other malicious activities like spamming or cryptocurrency mining.

Privacy Breaches and Data Harvesting

Many IoT devices collect vast amounts of personal and sensitive data—ranging from health metrics (wearable devices) to location data (smartphones, connected vehicles). If poorly protected, this data is ripe for theft, misuse, or unauthorized surveillance.

Device Spoofing and Impersonation

IoT devices often interact in automated networks, communicating with each other and external systems. Attackers can spoof IoT devices to impersonate legitimate ones or manipulate the flow of data, leading to inaccurate data being fed into systems that rely on it for decision-making.

Weaknesses in IoT Device Integration

IoT devices are often integrated into a wide variety of ecosystems, such as smart homes, manufacturing systems, or hospitals, creating a complex web of interdependencies. A vulnerability in one IoT device can cascade and impact other connected devices in the ecosystem.

Ransomware as a Service

Explosion of Ransomware Attacks from Inexperienced Threat Actors

The availability of RaaS will democratize ransomware attacks, enabling a wide range of individuals, including non-technical criminals, to participate in cybercrime. RaaS providers typically offer user-friendly interfaces and customizable malware tools, meaning almost anyone can become a ransomware operator with minimal expertise.

Hyper-Personalized & Sophisticated Campaigns

RaaS operators often provide attackers with advanced tools and tactics that allow them to tailor ransomware campaigns for maximum effectiveness. Attackers will be able to leverage AI-powered ransomware and deep learning algorithms to create campaigns that are hyper-targeted, highly personalized, and difficult to detect.

Rise in Double and Triple Extortion Models

RaaS will integrate more extortion methods into their offerings, pushing attackers to adopt double or triple extortion techniques. Attackers not only encrypt the victim's data but also threaten to release sensitive information publicly if the ransom isn't paid. Triple extortion goes a step further by also attacking a third party connected to the victim.

Expansion of Ransomware Targeting Critical Infrastructure

RaaS will enable more cybercriminals to target high-value sectors like healthcare, finance, energy, and government—critical infrastructure that relies heavily on operational technology (OT). With increasingly automated attack tools and better strategies for infiltrating OT networks, these attackers will be able to cripple operations, causing disruption, financial loss, and national security risks.

Cyber Skills Gap

Increasing Digital Transformation and IT Complexity

Technology is advancing at a rapid pace, and organizations are adopting new tools, platforms, and systems (e.g., cloud technologies, IoT, AI-driven systems). However, the speed of these advancements can leave cybersecurity teams struggling to stay current on best practices, vulnerabilities, and security solutions.

Insufficient Cybersecurity Education & Training Programs

There are insufficient cybersecurity education programs to meet the growing demand. Despite the increasing recognition of the need for skilled professionals, the education system has not kept pace with the complexity and volume of emerging cybersecurity challenges.

Burnout Rates Among Cybersecurity Professionals

The high volume of cyberattacks and the pressure to protect increasingly complex systems is leading to burnout among cybersecurity professionals. This results in high turnover rates, further exacerbating the skills gap.

Global Competition for Cybersecurity Talent

As the global demand for cybersecurity professionals grows, countries and companies will increasingly compete for the best talent. This leads to higher salaries, increased demand for workers with niche skills, and talent migration to organizations with the most resources to attract and retain top professionals.

Supply Chain Interdependencies

Third-Party Vendor Breaches

As organizations increasingly rely on third-party vendors for various services (cloud services, software, hardware, IT support, etc.), each of these vendors presents a potential attack surface. Vulnerabilities in a single supplier's infrastructure can easily lead to a domino effect across the entire supply chain.

Software Supply Chain Attacks

The software supply chain has emerged as a particularly vulnerable target for cybercriminals in recent years. Cyber attackers often compromise popular software libraries, platforms, or tools that are used by multiple organizations, making the attack highly scalable.

Ransomware Targeting Supply Chain Dependencies

Ransomware attacks increasingly target the critical suppliers in an organization's network, locking down operations not just for the immediate victim but also for other dependent companies further down the chain.

Inadequate Risk Management and Monitoring

Many organizations do not have a comprehensive view of the security posture of their entire supply chain, especially when it comes to third-party vendors or subcontractors. This lack of visibility makes it difficult to assess and mitigate risks effectively, leaving critical vulnerabilities exposed.

Regulatory Requirements

Increased Compliance Costs

Organizations will face growing pressure to comply with an expanding array of local, national, and global regulations related to data protection, privacy, and cybersecurity. This often means more resources will need to be dedicated to ensuring compliance, including investments in security technologies, staffing, and training.

Impact on Innovation and Business Agility

As companies implement tighter security measures and compliance frameworks, the time-to-market for new products and services could be affected. Businesses will have to incorporate security by design, including making sure they comply with regulations such as NIST, ISO 27001, or regional laws like California's CCPA.

Heightened Risk of Non-Compliance Penalties

As regulations become stricter in 2025, the risk of non-compliance will increase, and the penalties for violations will become more severe. Regulatory bodies will be empowered to impose hefty fines, potentially crippling businesses that fail to comply with rules.

Integration of Privacy & Security Controls into Business Models

Businesses will need to integrate security and privacy controls into their business models by default (also known as security by design and privacy by design). This means incorporating robust data protection policies, encryption, access controls, and auditing features right from the early stages of product and service design.

Cloud Security Challenges

Misconfigurations and Human Error

Misconfigurations remain one of the top reasons for cloud security breaches. With complex cloud environments involving multiple cloud service models (IaaS, PaaS, SaaS) and various settings, misconfigured services (e.g., public-facing storage buckets, databases, or overly permissive access controls) expose sensitive data.

Data Privacy and Compliance Challenges

In 2025, organizations will face more stringent data privacy regulations (e.g., GDPR, CCPA, China's Personal Information Protection Law) as well as increased concerns around data sovereignty. These regulations place specific requirements on where and how data is stored, and organizations that don’t comply may face hefty fines.

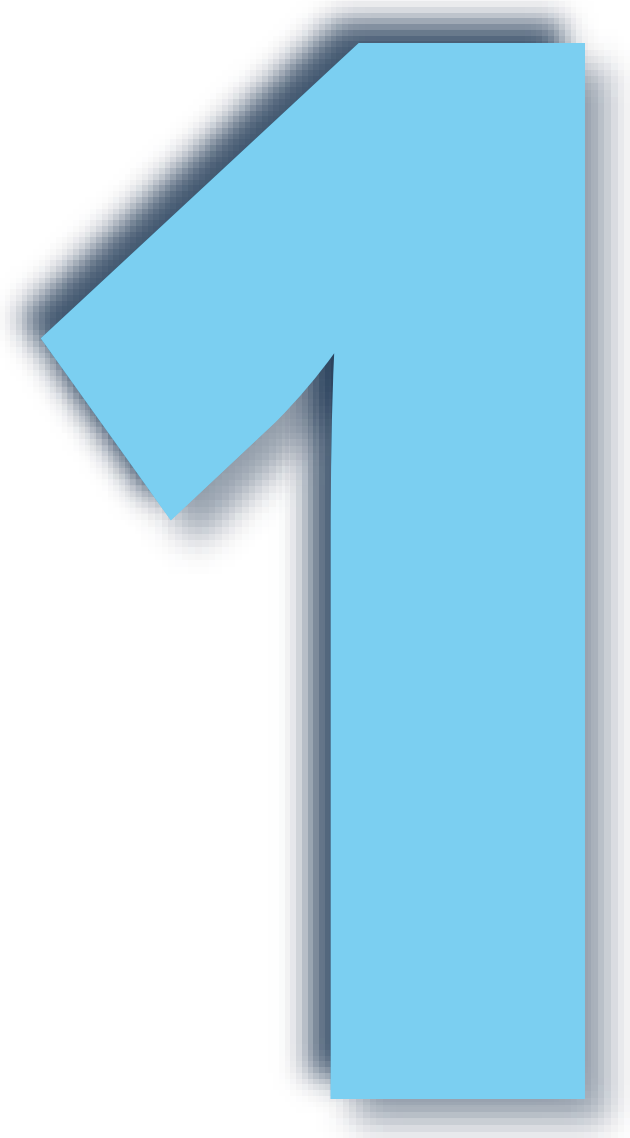
Cloud-Native Application Vulnerabilities

With the rise of cloud-native technologies such as containers, microservices, and Kubernetes, the attack surface is further expanding. These environments are highly dynamic and securing them requires specialized knowledge and tools.

Increased Attack Surface with Multi-Cloud & Hybrid Environments

Many organizations are adopting multi-cloud and hybrid cloud environments (using services from multiple cloud providers like AWS, Azure, and Google Cloud), which makes it more challenging to maintain consistent security policies and controls across different platforms. This results in an expanded attack surface.

Define Your Journey



Set Your Objective

- ISO 27001
- Cybersecurity Maturity Model Certification (CMMC)
- NIST Cybersecurity Framework (CSF)
- Systems and Organizational Controls (SOC) 1/2

Create Awareness

- Security Training & Testing
- Threat Research & Intelligence
- Continuous Monitoring
- Continuous Assessment

Adopt a Zero Trust Architecture

- Identity & Access Management
- Micro-Segmentation
- Device & Endpoint Security
- Data Protection & Encryption
- Automation & Orchestration

Be Vigilant

- Leadership & Governance
- Establish a Security Culture
- Risk Management & Assessment
- Technology & Tools
- Cyber Resilience - Incident Response, Recovery & Reporting
- Vendor & 3rd Party Risk Management

SilverTree

Thank you

SILVERTREESERVICES.COM

Darwin Herdman
General Manager