

ANOMALI

REPORT

---

# Top 10 Cybersecurity Trends



# Always Stay One Step Ahead

The most challenging thing about cybersecurity is the very thing that makes it the most interesting and dynamic discipline in the world of IT: it's a cat-and-mouse game that never ends. Attacks grow increasingly sophisticated, especially in the age of AI. The charter of the cybersecurity professional is to outthink the adversary — to always stay one step ahead. The stakes are incredibly high, since a single breach can put vast amounts of personal information at risk and destroy a company's reputation in the space of minutes. This report covers the top 10 most important cybersecurity trends and challenges facing the enterprise and provides proactive guidance.

## 1. AI Attacks Are Proliferating at an Alarming Rate

The last two years have seen an accelerated adoption of AI. While most organizations are leveraging these tools to streamline systems (and even to bolster security), malicious actors are also availing themselves of these technologies to increase the effectiveness of their arsenals.

Here are a few examples of AI attack techniques that are becoming more frequent:

### Input Attacks

Adversaries armed with AI are often up against security systems availing themselves of similar technology. Input attacks are designed to exploit the vulnerabilities and limitations in the target systems' machine learning models with inconsistent data sets to produce incorrect or undesirable results. In essence, they confuse the AI defenses with unexpected input.

### Poisoning Attacks

This technique relies on inserting malware into target systems when the AI defense system is created. The goal is to cause the target system to malfunction in a way that the attacker intends, making it exploitable. Poisoning attacks often work by corrupting data, which, in turn, compromises machine learning models.



## Evasion Attacks

This technique involves exploiting vulnerabilities in the model's algorithm to escape detection.

### What To Do About It

The three types of attacks detailed above are all AI attacks exacted upon AI systems. While AI adoption has proceeded at a dizzying pace, staying abreast of the architecture of AI threats will help your team build safeguards into your systems. This goes for all AI systems, not just AI defenses. Always look for the Achilles' heels and plug the holes before deployment. The key here is intentionality. Consider forming cross-functional groups to track adoption, contingencies, and dependencies. Include development, finance, sales/marketing, operations, and customer support teams.

## 2. Dark Data Is Getting Bigger and Darker

Estimates from IBM (and others) categorize as much as 80%+ of an organization's data as being "dark" — unstructured, redundant, inaccurate, or unused. The amount is growing exponentially, thanks to the rise of Internet of things (IoT) and operational technology (OT). Aside from the obvious waste of storage resources, this dark data poses significant security and compliance risks<sup>1</sup>. This is going to be tough to get ahead of, but it is very much in your interest to do so.

### What To Do About It

Start with an IT audit mapped to your potential attack surface to identify and track potential exposure points. Look at how system resources are being used and look for dormant files. (Given how vast the datasets are, this may be a task best delegated to an AI application.) Consider making this an ongoing activity, since the amount of data you have is only going to increase.

## 3. Increased focus on Zero Trust Architecture

Zero Trust Architecture (ZTA)<sup>2</sup> is gaining momentum as organizations move away from traditional perimeter-

### What To Do About It

While this can be annoying to users (because they have to keep verifying their identities), it's too important to neglect. While IT will be the group to implement enforcement protocols, the marching orders for this should come from your CISO, to avoid the inevitable pushback.

## 4. Expansion of IoT Security Concern

While IoT is not new, devices are becoming increasingly sophisticated. As a result, they are generating more data, which expands their attack surfaces and makes them more attractive targets. This sets the stage for particularly onerous attacks: hacking into a hospital and changing the settings on a critical medical device, hacking home security systems, hacking into an automobile computer while someone is driving, and so on.

### What To Do About It

Because IoT has a heavy presence in OT, IT and OT teams need to align — particularly around integrations and workflows. Start with an attack surface audit that goes beyond traditional IT infrastructure and covers OT and industrial control systems (ICS). A comprehensive audit will give you a clear picture of what's in place.

## 5. Heightened Regulatory Compliance

Compliance mandates exist to ensure that corporations pay adequate attention to protecting data and privacy in the context of preventing threats<sup>3</sup>. These laws — which are dense, opaque, nit-picky, and subject to retroactive enforcement — are expected to increase in strictness and complexity over the coming years.

### What To Do About It

It makes sense to have someone on the executive level of your company focused on compliance. That person should work hand-in-hand with your in-house counsel, who should, in turn, be backed up by a law

<sup>1</sup> <https://www.anomali.com/blog/shining-a-light-on-dark-data>

<sup>2</sup> <https://www.anomali.com/blog/threat-intelligence-is-a-core-component-of-a-zero-trust-architecture-zta>

<sup>3</sup> <https://www.anomali.com/blog/the-sec-wants-more-transparency-from-the-companies-it-oversees>



firm that specializes in compliance. Because regional or domain requirements tend to be very specific (CPRA vs. GDPR vs. HIPAA, etc.), you may need multiple firms. These services do not come cheap, but are much less expensive than the fines you'll incur if you violate the law.

## 6. Increased Focus on Supply Chain Security

Most commercial software packages rely on at least some open source components. Because open source software may have hundreds or even thousands of authors, it is not as easy to “police” as code developed by a single manufacturer. Supply chain vulnerabilities present significant risks to organizations, their partners, and their customers. It's such an important issue that President Biden issued an executive order on May 12, 2021, requiring software and FedRAMP vendors to follow a number of best practices, including providing software bills of materials (SBOMs) to increase transparency and employing automated tools to check for known and potential vulnerabilities and remediate them. Because supply chain insecurity is likely to increase, along with the complexity of infrastructure and the wide availability of AI, it should always be top of mind.

### What To Do About It

Look into vendors' security practices and history before integrating third-party components. Conduct regular security audits of suppliers and require them to provide SBOMs. Always install regular security updates and patches. Ensure that compliance and security teams conduct regular audits.

## 7. Accelerating Shift to Cloud Security

The widespread adoption of cloud computing is already leading to an increased focus on cloud security strategies and, specifically, the need for a more robust cyber threat intelligence (CTI) response. The increasing urgency for the implementation of CTI in an organization's security posture marks a maturation from reactive to proactive security strategies driving two crucial strengths — preparedness and resilience. Going forward, companies will be able to gain a much better

understanding of adversaries' tactics, techniques, and procedures that will enhance the protection of their cloud environments.

### What To Do About It

Expect to see the industry making a much bigger investment in tools and technologies to secure cloud environments and data stored in the cloud. If your company doesn't have a CTI program in place, it's a good time to create one. To ensure that your CTI data correlates with data tracked in your SIEM, your SecOps team should align with your CTI team.

## 8. Cybersecurity Skills Gap

Analysts are tasked with processing hundreds of IOCs per day — each requiring at least 20-30 minutes of painstaking work to review. If you add in the potential downside of letting something unintentionally slip through, you'll easily see why analyst burnout and turnover is a real issue. To make matters worse, the role requires significant skill, including a knowledge of specialized query languages, which is often beyond the reach of relatively junior security analysts. The combination of factors means that the shortage of skilled cybersecurity professionals will continue for the foreseeable future.

### What To Do About It

While it's critical to invest in training and education programs for existing analysts, it's also important to look into AI technology that employs natural-language processing to prioritize threat insights to augment analysts' knowledge. Tools like these can reduce the effort required for analysts to do their work, which, in the long run, may narrow the coverage gap.

## 9. Increased Cyber-Physical Security Integration

As operational technology (OT) and industrial control systems (ICS) become more interconnected with IT systems, the potential attack surfaces expand exponentially and the risk of operational disruption increases. So do cross-domain threats (malware originally targeting IT systems), which spread laterally



across interconnected systems. Going forward, the convergence of cyber and physical security will become increasingly important to protect critical infrastructure. This is already happening on larger and larger scales. Similarly to the effects of IoT breaches, attacks on critical infrastructure start to hit very close to home, compromising utilities, traffic control systems, and so on.

## What To Do About It

This is very similar to securing your supply chain or IoT infrastructure. IoT and OT have a significant overlap, and most of this is spread across your supply chain. Start with an audit to get a clear sense of how much work your team is facing, correlate this information with both operational and partner teams, manage it through your CISO's organization, then update on a regular cadence.

## 10. Continued Evolution of Threats

Cyber attacks will continue to evolve and grow more sophisticated. Expect to see more Advanced Persistent Threats (APTs), which will target critical infrastructure. This infrastructure is increasingly interconnected and therefore presents an attractive target. APT groups will escalate their efforts to infiltrate and disrupt critical infrastructure sectors (such as energy, transportation, and healthcare) using zero-day exploits, supply chain attacks, and covert network infiltration, posing significant challenges for detection and mitigation.

We'll also be seeing more ransomware targeting cloud

environments and IoT devices. Cloud services and IoT ecosystems present lucrative targets for ransomware operators due to their widespread adoption and potential impact on business operations and personal privacy. Future ransomware variants will exploit vulnerabilities in cloud infrastructure, misconfigured IoT devices, or weak authentication mechanisms to gain unauthorized access and encrypt critical data, creating challenges for incident response and recovery.

We'll also be seeing an escalation in AI-powered cyber attacks and deepfakes. The integration of AI/ML into cyber attack tools and techniques will pose a significant threat. Malicious actors are leveraging AI to automate and enhance various stages of the cyber attack lifecycle, including reconnaissance, evasion, and obfuscation.

What's more, the proliferation of deepfake technology raises concerns about the manipulation of digital content for malicious purposes, such as creating convincing impersonations or spreading disinformation campaigns. These nefarious activities will spike during times of national elections and geopolitical uncertainty.

## What To Do About It

This is about as complex as it gets. To address these threats, organizations must immediately prioritize cybersecurity investments in areas such as threat intelligence, threat identification, correlation, and remediation. They must also invest in vulnerability management, secure software development practices, and continuous employee training.

## Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. [Request a demo](#) to learn more.





Mollam aut omnis eos sam simporeperit volo et ea dem repudanda consed eossequam saperum alitia seque ma nate volluptatur simoluptatur am ut accatur, experum recaetur, tem. Obitatet eturit atemquis rem voluptibus assunt quo optio dolupti re soluptae pero vel illaborias est, vollaccuptas nos non esequia cus rehendipsam idenese quunte demquos nis et ullestia qui blab intus, quo doluptatis eati corum volo torrorp oribus pientur sam quibus, sandit voluptati consediam qui con pa quam re, sum quamet et qui blam ium restrum quas rescilitibus est quatia pel eumquodi optame essenda erchita vel et aut qui omnis quo et eostior erionemqui dolecatem exerspe lecerna tempelit elestrum la conectum, odionsecae pa debis volut exerumque valoribusam, omnis que culparum, qui aut qui doluptasit ut reprori tibus, comnis eturepe lliqui vel iniende ntotat as rehento ducid quis ma consequis et veligenis ant dolupta temquia sitate voluptamus essumet, culluptam eumquo maximus di cor magnis vel idit ut rem lautenist inctorerro offic tenihil ide nusam, que latus, ut doluptat am lit renihit la velessusae. Nequi offic te pa sed mi, nia vit quiderum que doluptas sunt moluptas volorec earcitame restemo luptus apid que volut untent volupta tionsed earia videm et, et et faciend iasitis quam num alit que etus re ea doluptatin conse culparc hilluptias non prae occulparum volorum, eos et modia volorepro quiaest at vent.

Puda et iunt oditacte ommolupta id quidenis as voluptus autempo rporestem quam elibus dis delit, sitasperias ma sa consequ iasperum ipsum ad quiatus, inctotatur? Ab inum aturit fugias di dolore omnit esti

berumet latatem volo explaborunt.

Gia que exces enda velis voles volecae poreribus ipsapelecae corporem que nam ratur? Omnihit quam litatin ctorate mquiatem. Ut mo cum et aut qui to ex et ut lam quatur, explaborro temporibus, volessimeni omnitiis simus ea dicum rem que lam sam et etur, et estrum exped endus sam aligend itistibus audandi scipsum doluptum solum si bero officil ligenih iciaspid modignam etur, con explamet eles aut volesed exceria ssequaturit qui doles aut facius quas pratur, si sum fugiate mo cus.

Piendi qui ommod qui officipit fugia denim lant unte eveliti aecesci endaece perate intur? Quibus nisti untur rem re pernatur, intiis inctusae. Nequi doloruptaque et eaquantium que officitas voluptae nimust apiducia volendis nonsenda voluptae volupta tquiduc ipitaqui rae consecatum, susapientum cus quibus.

Um et earuptiur, vollor sit vel idunt porro erum et evenderi sequodi volupta eptataquam iducimp ostrum eos molesed unt quis quaspel exceptas perit, soluptiat erepeles eate omnimuscia nihitiu ribusa conestem rata quiate nostest officae pudigna tessund ignatia nonsequamet quostis et quidescitae cuptinv eleseque volut evelendis voluptatiunt quasitia nectaqu iducit aris asperunt veliquasse pratent, cum recuptius natioos usapid mo quam velestiis dolorum, ommos simusto etur? Quis et volut omnis andel idio consequi odit la dolupta spedia sequam volupta dolorum la nos praestio et mi, sit, quia denis dolorepeles doluptur, qui numquam nest accullorum net hilla dis explibea quo cus nesedi anduciatursusdam sitaqui nosapid molliquos enihil in

## Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. [Request a demo](#) to learn more.