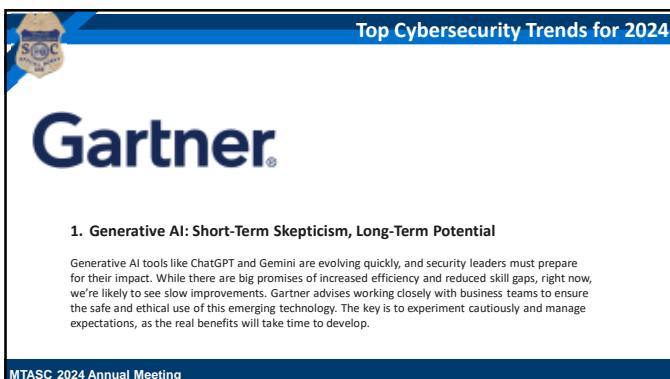


The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina.

Consult your attorney for advice concerning specific situations.







Top Cybersecurity Trends for 2024



Gartner®

2. Outcome-Driven Metrics: Improving Communication with the Senior Leaders

Cyber incidents are becoming more frequent, making executives question their cybersecurity strategies. Outcome-driven metrics (ODMs) help bridge this gap by clearly showing how security investments translate into protection. These metrics are essential for justifying cybersecurity spending and showing non-technical executives how risks are being managed in a simple, understandable way.

MTASC 2024 Annual Meeting

Top Cybersecurity Trends for 2024



Gartner®

3. Security Behavior and Culture: Reducing Human Risk

Focusing on changing employee behavior, rather than just raising awareness, is becoming a key strategy to reduce security risks. By 2027, half of large companies will design security practices around human behavior to reduce friction and improve compliance. Programs that build a culture of secure behavior are helping employees adopt better security habits, making them more independent in managing cyber risks.

MTASC 2024 Annual Meeting

Top Cybersecurity Trends for 2024



Gartner®

4. Resilience in Third-Party Risk Management

Security leaders are shifting focus from checking third-party vendors upfront to ensuring long-term resilience in case these partners face security issues. This means developing better contingency plans and working closely with external partners to safeguard critical assets. Gartner suggests creating incident response strategies specific to third-party risks, including clear offboarding processes when partnerships end.

MTASC 2024 Annual Meeting

Top Cybersecurity Trends for 2024



5. Continuous Threat Exposure Management: Reducing Breaches

Continuous Threat Exposure Management (CTEM) involves constantly assessing how exposed an organization's digital and physical assets are to threats. By focusing security efforts on specific threats or projects, organizations can identify and address vulnerabilities faster. By 2026, companies that prioritize this approach are expected to see a significant reduction in breaches.

MTASC 2024 Annual Meeting

Top Cybersecurity Trends for 2024



6. Expanding Identity & Access Management (IAM) for Better Security

As companies shift to an "identity-first" security approach, Identity & Access Management (IAM) is becoming more critical. Instead of focusing only on traditional network security, the emphasis is on properly managing who can access what. Gartner advises that organizations strengthen their IAM systems to improve overall security resilience, including better detection and response to identity-based threats.

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

8 Most Common Causes of Data Breaches in 2024

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

Weak and Stolen Credentials
Weak or stolen passwords remain one of the top causes of data breaches. Even though hacking gets the most attention, many attacks succeed because hackers exploit easy-to-guess or compromised credentials. In fact, 80% of breaches are linked to weak or stolen passwords.

Key Takeaways

- According to the 2023 Verizon Data Breach Investigations Report, 83% of breaches were caused by external attackers, with 49% of those involving stolen credentials.
- Over 15 billion stolen credentials are available on the internet and dark web, according to the Digital Shadows Photon Research team.
- 50% of retail cyberattack victims face extortion, while 25% have their credentials stolen.

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

Backdoor and application vulnerabilities
Cybercriminals often exploit weaknesses in software or poorly designed systems to gain unauthorized access to sensitive data. These vulnerabilities act as open doors, allowing hackers to bypass security measures and steal valuable information.

Key Takeaways

- Web application attacks account for 26% of all breaches, making them the second-most common attack type.
- Over 60% of all bot traffic on the internet is driven by malicious bots.
- 17% of cyberattacks specifically target weaknesses in web applications.
- In the digital commerce sector, 75% of fraud and data theft happen through web application vulnerabilities.
- Application-layer attacks surged by 80% in 2023, with over 25,000 vulnerabilities (CVEs) reported.
- 18% of websites are infected with severe threats like backdoors and malicious file modifications.

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

Malware
Malware is malicious software that is unknowingly installed on systems, giving hackers access to exploit not only the infected system but also any connected ones. This poses a serious security risk, as malware can steal sensitive data for financial gain or cause further harm to an organization's network.

Key Takeaways

- In 2023, hackers launched an average of 11.5 attacks per minute, including 1.7 new malware samples per minute, according to Parachute.
- 92% of malware was delivered through email or by uploading files to external systems.
- The first half of 2023 saw 2.8 billion malware attacks, with over 270,000 never-before-seen variants discovered.
- Around 30% of malware breaches come from emails containing fake links and attachments.


MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

Social engineering
 Instead of hacking systems directly, cybercriminals use social engineering to trick people into giving them access. This involves tactics like phishing emails, phone scams, or malicious links sent via email, text, or social media, where individuals unknowingly share sensitive information like login details.

Key Takeaways

- Social engineering is involved in 98% of all cyberattacks.
- Verizon's 2023 report states that 10% of security incidents and 17% of data breaches are caused by social engineering.
- The average organization faces more than 700 social engineering attacks each year.



MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches


Too many permissions
 When companies grant excessive or outdated access permissions, it creates opportunities for hackers to exploit. If businesses don't strictly manage who can access what, insider threats and security breaches become more likely, as unauthorized individuals may have access to sensitive information.

Key Takeaways

- Remote and hybrid work models are becoming more common, with 16% of companies operating fully remotely and nearly all employees wanting some remote work options.
- Gartner predicts that by 2026, only 10% of large enterprises will fully adopt the Zero Trust security model, but less than 1% have done so today.
- Phishing remains the most common cybercrime, with 3.4 billion malicious emails sent daily in 2023.
- Business Email Compromise (BEC) attacks doubled in 2023, reaching 10.77 attacks per 1,000 mailboxes, peaking at 14.57 per 1,000 in October.
- Phishing attacks cost businesses an average of \$4.9 million per incident, according to IBM.

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches



Ransomware
 Ransomware is malicious software that blocks access to a computer system or files until a ransom is paid, usually in cryptocurrency. It encrypts the victim's data or locks their system, making it unusable, and demands payment to restore access.

Key Takeaways

- Ransomware attacks are becoming more frequent and sophisticated and are expected to remain a dominant form of cybercrime in 2024.
- In 2023, ransomware was the motive behind more than 72% of cybersecurity attacks, according to Statista.
- IBM reported a 41% increase in breaches caused by ransomware, and these attacks took 49 days longer than average to detect and contain.
- The average ransom in 2023 was \$1.54 million, nearly double the \$812,380 average in 2022.

MTASC 2024 Annual Meeting

8 Most Common Causes of Data Breaches

Improper Configuration and Exposure via APIs

Misconfigurations, such as default passwords, open ports, or weak encryption, create security gaps that hackers can exploit. APIs, which handle a large portion of web traffic, are especially vulnerable when not properly configured. Failing to secure APIs and misconfigured systems can lead to unauthorized access and data breaches.

Key Takeaways

- The number of unique API attacks increased by 60% between Q2 2022 and Q2 2023.
- APIs account for 83% of all web traffic, making them a top target for cyberattacks.
- The EMEA region saw the highest percentage of API attacks (47.5%), followed by North America (27.1%) and APJ (15%).
- A report by VentureBeat found that 41% of organizations experienced an API security incident in the last year, with 63% of those leading to a data breach or data loss.

MTASC 2024 Annual Meeting


8 Most Common Causes of Data Breaches

DNS Attacks

DNS attacks target the system that translates domain names into IP addresses, causing disruptions or redirecting users to malicious sites. These attacks can lead to service downtime, unauthorized access, or the exposure of sensitive data.

Key Takeaways

- In 2023, 90% of organizations experienced a DNS attack, according to the IDC DNS Threat Survey.
- On average, organizations faced 7.5 DNS attacks, each costing around \$1.1 million.
- 73% of affected organizations reported application downtime due to DNS attacks.



MTASC 2024 Annual Meeting

AI and LLM


Artificial Intelligence and Large Language Models

MTASC 2024 Annual Meeting

AI and LLM

The benefits of AI

- Increased levels of efficiency
- Automate many manual tasks
- Helps alleviate burnout
- Your own personal assistant and expert in everything




MTASC 2024 Annual Meeting

AI and LLM

In June of 2024, The South Carolina Department of Administration published the South Carolina State Government's Artificial Intelligence (AI) Strategy.

The strategy is rooted in the three Ps: **Protect, Promote and Pursue**—outlines the state's AI vision, guiding principles, goals and actions necessary for the productive and responsible use of AI for state agencies.

The strategy also outlines several critical initial steps, including the establishment of an agency-staffed Center of Excellence (COE) and an AI Advisory Group to assist state agencies as they evaluate the use of AI.



MTASC 2024 Annual Meeting

AI and LLM

78%
Of AI users bring their own AI tools to work

52%
Of people who use AI at work are reluctant to admit to using it for their most important tasks.

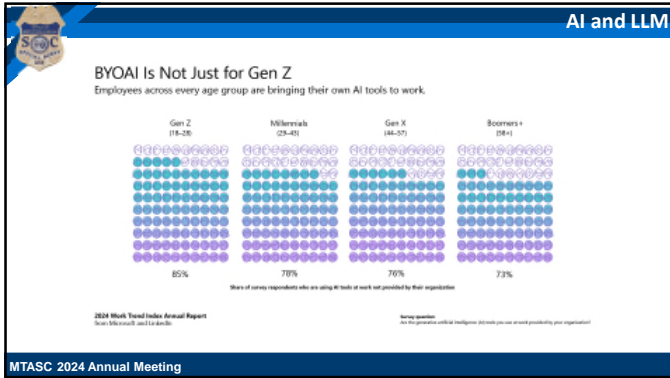
46%
Of them just started using it less than 6 months ago

68%
Of people say they struggle with the pace and volume of work

85%
Of emails are read in under 15 seconds, and the typical person has to read about 4 emails for every 1 they send

60%
Of workers time is spent on emails, chats, and meetings

MTASC 2024 Annual Meeting



AI and LLM

Using AI is not without risks

- **Overreliance**
Relying too heavily on tools like ChatGPT can be risky because changes to the tool—like a drop in performance or restrictions on the free version—can disrupt daily work. Since companies like OpenAI control these AI systems, businesses that depend on them might face problems if key functions suddenly stop working or become paid services. To avoid disruptions, businesses should have backup plans and not rely solely on AI tools.
- **Hallucinations**
AI sometimes generates completely made-up information, a phenomenon called "hallucination." A well-known example involved a lawyer submitting fake legal cases generated by AI. These errors can be hard to catch, and verifying AI-generated information can be time-consuming, defeating the purpose of using the tool for efficiency. To prevent the spread of false information, companies need to train employees on how to use AI responsibly and verify its outputs.

MTASC 2024 Annual Meeting


AI and LLM

Using AI is not without risks

- **Data Security**
Major companies like Amazon and Microsoft have warned against entering sensitive information into AI systems like ChatGPT, as there's uncertainty about how the data is handled. Even if data is used anonymously, it could still expose confidential or proprietary information. Businesses must enforce strict data security policies and train employees on best practices when using AI tools to avoid potential data leaks or legal issues.
- **Dehumanization**
AI-generated content often feels impersonal and unnatural, which can harm communication. People can usually tell when something is written by a machine, which can leave them feeling disconnected. To maintain a personal touch, companies should guide employees on when and how to use AI for communication and ensure that human elements are retained in important interactions. A well-defined communication strategy can help avoid this issue.

MTASC 2024 Annual Meeting

AI and LLM



Using AI is not without risks

- **Intellectual Property**
AI systems can sometimes produce biased or discriminatory content because they learn from the data they are trained on, which can include human biases. This can lead to unfair decisions or problematic communications if not monitored carefully. Businesses must be aware of this risk and ensure they implement regular checks to avoid relying on AI-generated content that could harm their reputation or cause legal complications.
- **Dehumanization**
When using AI to generate content or review work like computer code, it raises the question: Who owns the output? If you ask an AI to review or correct your code, does the ownership remain with you, or does the AI provider have rights to the results? This lack of clarity can lead to legal disputes, especially when proprietary information or intellectual property is involved. Businesses should carefully review the terms and conditions of AI tools to understand ownership rights and take steps to protect their intellectual property when using AI for sensitive work.


MTASC 2024 Annual Meeting

Significant Cyber Breaches

Significant Cyber Breaches in 2024 (mostly)

MTASC 2024 Annual Meeting

Significant Cyber Breaches



Records Breached: 7.6 million current and 65.4 million former customers



July 12, 2024, AT&T disclosed that the phone records of almost all current and former AT&T customers were stolen by hackers back in April. The breach affects AT&T customers and anyone an AT&T customer called or texted when the logs were stolen.

The involved data AT&T was storing on a third-party cloud storage company that was left poorly secured. It includes records of calls and texts – including information about who users called and texted, when, and for how long.

Nearly all AT&T cellular customers, mobile virtual network operators customers using AT&T's network are impacted, as well as AT&T landline customers who interacted with these cellular numbers between May 1, 2022, and October 31, 2022, and for a few customers from January 2, 2023, are also impacted.

MTASC 2024 Annual Meeting

Significant Cyber Breaches

Records Breached: 77 million

MOVEit, a Managed File Transfer (MFT) application that provides secure file transfer services used by thousands of organizations and government agencies, was hit with one of the largest breaches in 2023.

The CLOP malware gang was able to exploit a security flaw and deploy ransomware, leaking confidential data of 77 million individuals and over 2,600 companies globally. U.S. companies were hit the hardest – 78% of breached companies – including U.S. Department of Energy, Johns Hopkins, the University System of Georgia, and in Louisiana (LA), the Office of Motor Vehicles announced that anyone with an LA driver's license or ID card could have had their data stolen in the breach.

Total damages globally are upwards of \$12 billion.

MTASC 2024 Annual Meeting

Significant Cyber Breaches






Records Breached: 560 million

May 2024, over 560 million customer records, including order history, payment information, name, address and email data, were leaked online and offered for sale by hackers who infiltrated Ticketmaster's systems.

The company has sent emails to their customers, advising users to monitor their accounts and credit statements.

MTASC 2024 Annual Meeting

Significant Cyber Breaches


Records Breached: 49 million

May 2024, Dell was hit with a massive cyberattack that could affect their 49 million customers. Menelik, the threat actor behind the attack, openly revealed to TechCrunch that he extracted large amounts of data by setting up partner accounts within Dell's company portal.

After partner accounts were authorized, the hacker launched brute force attacks, sending over 5,000 requests per minute to the page continuously for nearly three weeks. Astonishingly, Dell remained oblivious to these activities. Following the barrage of nearly 50 million requests and successful data scraping, Menelik proceeded to alert Dell by sending multiple emails about the security vulnerability.

MTASC 2024 Annual Meeting

Significant Cyber Breaches





Ascension

May 8, 2024, a ransomware attack against Ascension, a Catholic health system with 140 hospitals in at least 10 states, locked providers out of systems that track and coordinate nearly every aspect of patient care. They include its systems for electronic health records, some phones, and ones "utilized to order certain tests, procedures and medications," the company said in a May 9 statement.

"I don't believe that anyone is fully prepared for a long-term process like this," he said. Most emergency management plans he's seen "are designed around long-term downtimes that are into one, two, or three days."

MTASC 2024 Annual Meeting

Significant Cyber Breaches


More than a dozen doctors and nurses who work for the sprawling health system said that patient care at its hospitals across the nation was compromised in the fallout of the cyberattack over the past several weeks.

Clinicians working for hospitals in three states described harrowing lapses, including delayed or lost lab results, medication errors, and an absence of routine safety checks via technology to prevent potentially fatal mistakes.

Ascension Nurse Marvin Ruckle in Wichita, Kansas, had a frightening experience. He nearly gave a baby "the wrong dose of narcotic" because of confusing paperwork. He's worked in the neonatal intensive care unit for two decades and said it was "hard to decipher which was the correct dose" on the medication record.

MTASC 2024 Annual Meeting

Significant Cyber Breaches



January 2024, Microsoft disclosed that a Russia-aligned threat actor was able to steal emails from members of its senior leadership team as well as from employees on its cybersecurity and legal teams. The attacks were by a group known as Midnight Blizzard, which has previously been connected to Russia's SVR foreign intelligence unit by the U.S. government and blamed for attacks including the widely felt 2020 breach of SolarWinds.

Customers known to have been impacted in the incident included multiple federal agencies, CISA confirmed. Through the compromise of Microsoft corporate email accounts, Midnight Blizzard has "exfiltrated email correspondence between Federal Civilian Executive Branch (FCEB) agencies and Microsoft," CISA said in an emergency directive.

The breach, which is believed to have begun in November 2023, saw hackers initially gain access by exploiting a lack of MFA (multifactor authentication) on a "legacy" account, Microsoft said.

MTASC 2024 Annual Meeting

Misinformation Wars


The Misinformation Wars

MTASC 2024 Annual Meeting

Misinformation Wars


The Justice Department has seized more than 30 web domains that it said were part of a broader, ongoing, surreptitious effort by the Russian government to influence the 2024 U.S. election and American public opinion, federal authorities announced Wednesday.

- vip-news.org
- acrossthehline.press
- mypride.press
- truthgate.us
- warfareinsider.us
- holylantheald.com
- lexominium.com
- honeymoney.press
- bid4work
- fox-news.top
- fox-news.in
- washingtonpost.pm



MTASC 2024 Annual Meeting

Misinformation Wars



An unsealed indictment unsealed in New York's Southern District accused two employees of RT, the Kremlin's media arm, of funneling nearly \$10 million to an unidentified company, described only as "Company 1" in court documents.


CNN has independently confirmed that "Company 1" is Tenet Media, which is a platform for independent content creators. It is self-described as a "network of heterodox commentators that focus on Western political and cultural issues," according to its website, which matches language contained in the newly unsealed indictment.

The Tennessee-based company that the Justice Department alleges was being funded by Russian operatives working as part of a Kremlin-orchestrated influence operation targeting the 2024 US election is Tenet Media, which is linked to right-wing commentators with millions of subscribers on YouTube and other social media platforms.

MTASC 2024 Annual Meeting

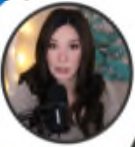

Misinformation Wars

"The company never disclosed to the influencers – or to their millions of followers – its ties to [Russian state media company] RT and the Russian government," US attorney general Merrick Garland said. His department described Wednesday's indictment as the most sweeping effort yet to push back against what it says are Russian attempts to spread disinformation ahead of the November presidential election.



MTASC 2024 Annual Meeting

Misinformation Wars

Tenet Media's US-based founders are not named in the indictment, but business records filed in Tennessee reveal two people connected to the company: Lauren Chen and Liam Donovan. A Twitter account for Donovan identifies him as the president of Tenet Media and his Instagram account describes Donovan as Chen's husband.

A private message between the two in May 2021 read, "So we're billing the Russians from the corporation, right?" Two weeks later, another message said, "Also, the Russians paid. So we're good to bill them for the next month I guess," the legal filing details.

Chen, is a rightwing online influencer in her own right. She has appeared in some of Tenet Media's videos and has more than 500,000 subscribers on YouTube.


MTASC 2024 Annual Meeting

Misinformation Wars

A former aide to New York Gov. Kathy Hochul and former Gov. Andrew Cuomo was charged with acting as an agent for the Chinese government.

Linda Sun, a former deputy chief of staff to Hochul and Cuomo aide, was charged with violating and conspiring to violate the Foreign Agents Registrations Act, visa fraud, alien smuggling and money laundering conspiracy, according to an unsealed copy of the indictment.

While working for state government, Sun influenced the messaging of high-level state officials regarding issues of importance to China, blocked Taiwanese government representatives from access to the officials, and obtained official New York State proclamations for Chinese government representatives without authorization.



MTASC 2024 Annual Meeting

Misinformation Wars



The Russian state-controlled media RT lists Chen as a contributor for several articles in 2021 and 2022. She is also linked to the conservative youth organization Turning Point USA. As of Thursday afternoon, Turning Point US had deleted webpages featuring Chen.

A YouTube video referenced in the indictment further describes Tenet Media as "a project of Lauren Chen and her husband Liam."

Blaze Media on Thursday said it had fired Chen.

BlazeTV, a subset of the Glenn Beck-founded conservative outlet, has since taken down a page that previously promoted content Chen produced for the outlet, including her show "Pseudo-Intellectual."

"Lauren Chen was an independent contractor, whose contract has been terminated," Tyler Cardon, the chief executive of Blaze Media, said in a statement to CNN. The news was first reported by Semafor.

MTASC 2024 Annual Meeting

Parting Thoughts

Parting Thoughts

MTASC 2024 Annual Meeting


Parting Thoughts

Are you prepared for multiple attacks?

What if you're dealing with one emergency and a major breach happens?

- Your city is an evacuation zone for a hurricane. As everyone evacuates, you get alerted of a verified ransomware incident.
- You have a cut fiber that cut access off to your primary data center and you have multiple cases of compromised credentials with those accounts sending emails compromising others.


MTASC 2024 Annual Meeting

 **Parting Thoughts**

Why does cybersecurity fail?

Cybersecurity fails because of a lack of adequate controls. No organization can be 100% secure. Cybersecurity teams must decide where, when and how to invest in IT controls and cyber defense. To do that, benchmark your security capabilities and identify gaps to fill and priorities to target.


MTASC 2024 Annual Meeting

 **Parting Thoughts**

Do not overlook the human element.

Cybercriminals have become experts at social engineering to trick employees. Making sure employees have the information and know-how to defend against attacks is critical.


MTASC 2024 Annual Meeting

 **Parting Thoughts**

Third-party logins

Have you tried to implement MFA for all users but getting pushback from third parties like vendors or volunteers? Do you require third parties to use MFA or are the standards different?

MTASC 2024 Annual Meeting

 **Parting Thoughts**

Shadow IT

Do you have shadow IT operations in your organization and how do you handle them when you find them? Are policies and procedures in place that IT and IS are involved or have some level of oversight for contacts with a technical component?

MTASC 2024 Annual Meeting

 **Thank you**

Sean Fay
Inspector General
SC Department of Social Services
sean.fay@dss.sc.gov



LinkedIn
<https://www.linkedin.com/in/sean-fay/>

Twitter / X
<https://x.com/JustaSean>

MTASC 2024 Annual Meeting
