SECURITY
SUITE

MIDYEAR

CYBER-RISK REPORT

2024

Kaseya

The cybersecurity world never slows down, constantly evolving to serve up new risks and novel cyberattacks every day. Keeping track of all of these developments can be a challenge, which is why we're here to help. Welcome to the Midyear Cyber-Risk Report 2024, your essential guide to understanding this year's pivotal cyber-risk trends.

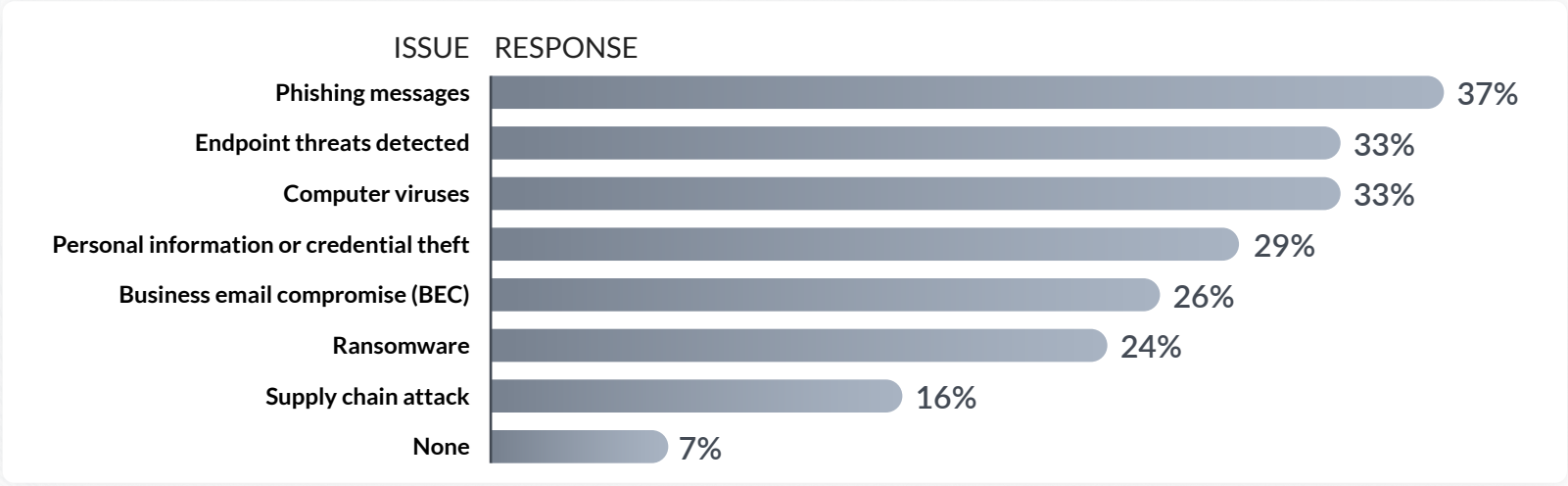
In this edition, we delve into the most notable risks that information technology professionals must grapple with to secure business systems and data. We'll explore the ways that artificial intelligence (AI) has revolutionized cybercrime, examine the ongoing evolution of the cyber-risk landscape, look at the risks that IT professionals should be concerned about and scrutinize the escalating threats to global supply chains.

This report will help IT professionals navigate the cyber challenges shaping 2024 and ensure their organizations are prepared for the road ahead.

IT PROFESSIONALS FACE A STORMY SEA OF EVOLVING SECURITY CHALLENGES

To gain a clear picture of the issues IT professionals face in 2024, it's important to understand where we started at the turn of the year. We asked IT professionals about their cybersecurity experiences and challenges in the **Kaseya Security Survey Report 2023** and here's what they had to say.

WHICH OF THE FOLLOWING CYBERSECURITY ISSUES IMPACTED YOUR BUSINESS IN 2023?

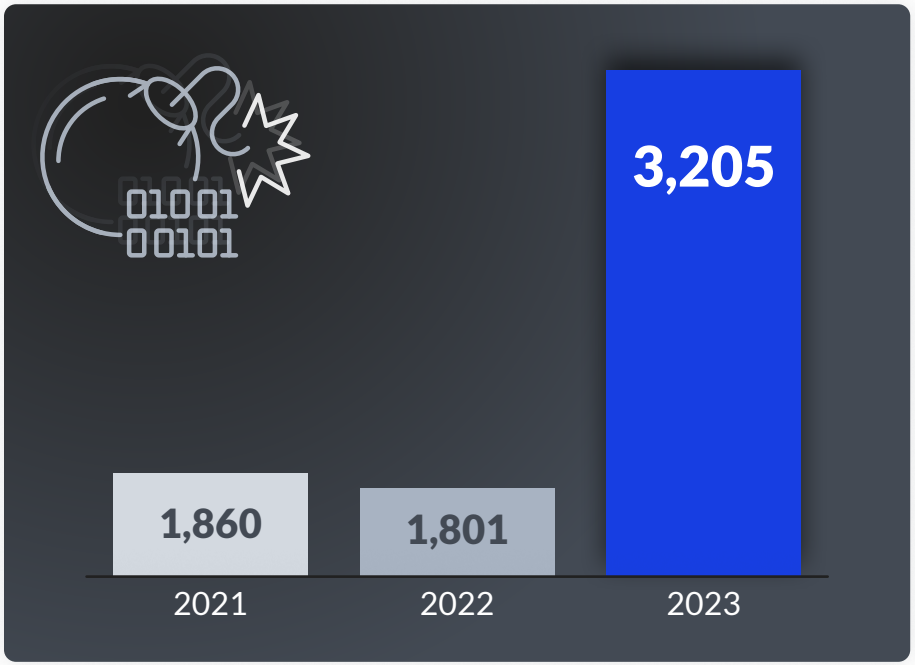


Source: Kaseya Security Survey Report 2023

DATA COMPROMISES ARE AT AN ALL-TIME HIGH

We've seen a concerning rise in the number of publicly reported data breaches. The U.S. hit a record high of **3,205 data breaches** in 2023 — a 78% increase from the previous year. And it doesn't seem to be slowing down. In the first quarter of 2024 alone, there were 841 reported breaches, up 90% from the same period in 2023. These figures highlight the critical importance for businesses to keep their cybersecurity strong to protect against data theft.

DATA COMPROMISES IN THE PAST THREE YEARS

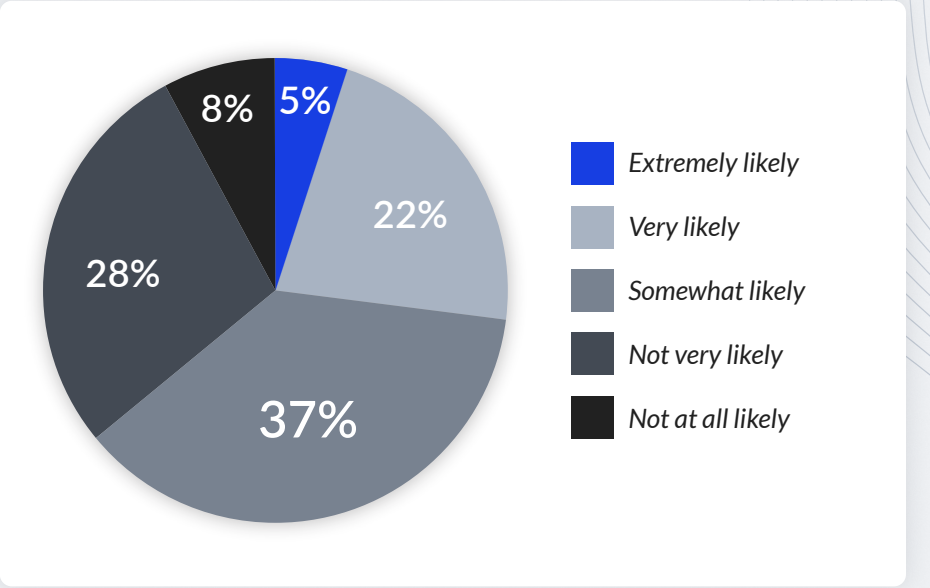


Source: ITRC 2023 Data Breach Report

MOST IT PROS EXPECT THEIR ORGANIZATION TO BE HIT BY RANSOMWARE IN 2024

Ransomware remains a significant and ongoing danger to businesses everywhere. Every day, cybercriminals find new ways to use cutting-edge technology, including generative AI, to create new and more sophisticated ransomware and malware. Alarmingly, 64% of the people we surveyed anticipate their organization will face a ransomware attack this year.

WHAT DO YOU BELIEVE IS THE LIKELIHOOD YOUR ORGANIZATION WILL EXPERIENCE A SUCCESSFUL RANSOMWARE ATTACK IN THE NEXT 12 MONTHS?



Source: Kaseya Security Survey Report 2023

***1048 ransomware attacks** were recorded in Q1 2024, up 73% over the same period in 2023.*

ZERO-DAY EXPLOITS SOAR

A zero-day attack, which is a cyberattack that exploits previously undiscovered vulnerabilities, is a term that we're hearing more frequently. In 2023, Google observed **97 zero-day vulnerabilities** exploited in the wild. That's over 50% more than in 2022, when 60 were reported.

SEVERAL FACTORS HAVE CONTRIBUTED TO THE SURGE, INCLUDING:

An increasingly interconnected business world as traffic increases between organizations and specialized service providers.

Cybercriminals searching for new avenues of attack as businesses harden their security.

Slipshod maintenance and patching by overworked IT teams.

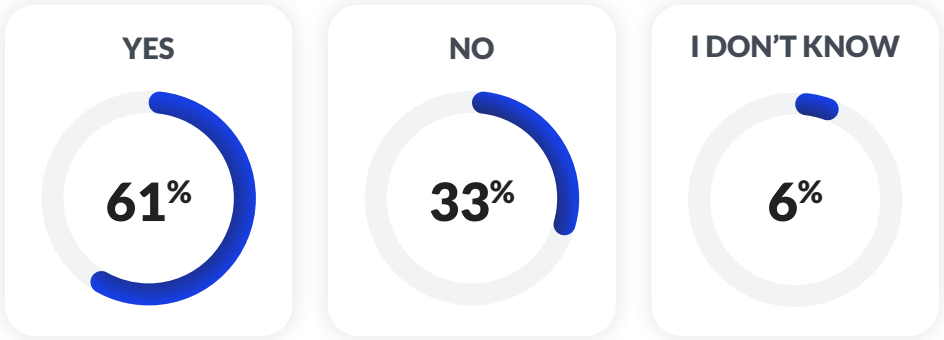
Modern software development practices that tend to result in common vulnerabilities.

Patch development focused on temporary mitigations rather than underlying causes.

SUPPLY CHAIN DANGER IS GROWING

Supply chain cyberattacks hit the headlines in 2023. In the U.S., these attacks affected **2,769 entities** — the highest since 2017. Sadly, 61% of the people we surveyed shared that their organization faced a cyberattack via their supply chain or a third-party service provider last year. This trend is on the rise, emphasizing the need for businesses to beef up their defenses in 2024.

HAVE YOU EXPERIENCED A SUPPLY CHAIN ATTACK THROUGH YOUR SUPPLIER OR SERVICE PROVIDER?



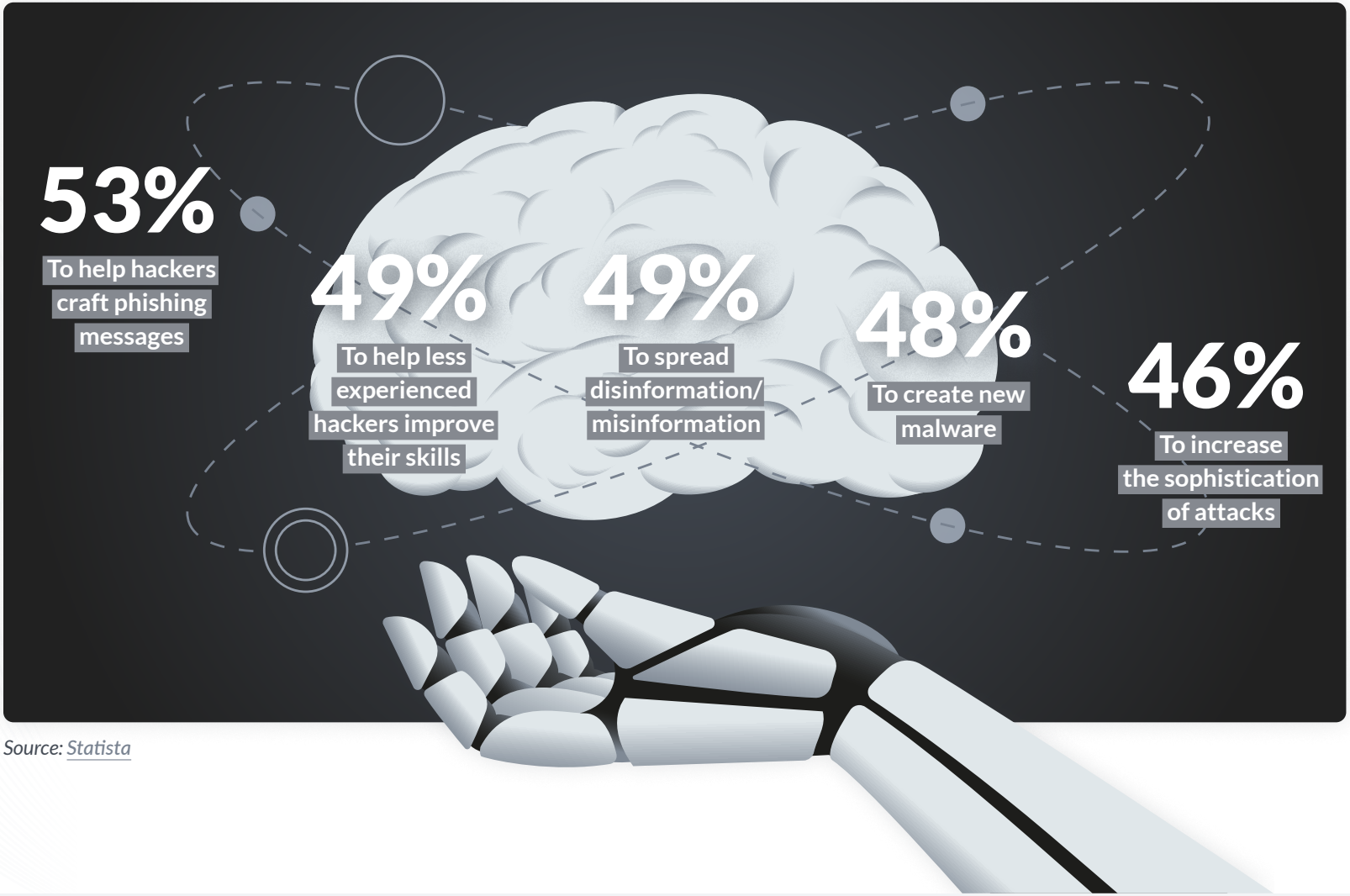
Source: Kaseya Security Survey Report 2023

***45% of global organizations** will experience a supply chain attack by 2025.*

AI HAS TRANSFORMED CYBERSECURITY

The AI revolution has made it easier for IT professionals to mount a strong defense with tools like AI-enhanced email security, antivirus and automated penetration testing. However, AI has also made it easier for bad actors to do their dirty work. **Microsoft warned** that over the last year, the speed, scale and sophistication of attacks has increased alongside the rapid development and adoption of AI as cybercriminals leverage the technology for their nefarious purposes.

WHAT ARE BAD ACTORS USING AI FOR?



Source: Statista

TREND 1: BUSINESS SERVICE PROVIDER ATTACKS THAT ROCK ENTIRE SECTORS

VICTIM:
Change Healthcare

FIRST REPORTED:
The Week in Breach News: 02/21/24 – 02/27/24

EXPLOIT:
Hacking

Our initial report: Change Healthcare is admitting that it experienced a successful cyberattack that caused widespread disruption to healthcare services and prescription processing across the U.S. The healthcare technology company is part of Optum and is owned by UnitedHealth Group. The trouble began on February 21, when bad actors were able to exploit the ConnectWise vulnerability. More than 100 Change Healthcare applications across pharmacy, medical record, clinical, dental, patient engagement and payment services were affected. Some reports are pointing to a state-sponsored threat actor as the culprit.

The aftermath: So far, this is the cyberattack story of 2024, with an impact that will reverberate for years. UnitedHealth, the parent company of Change Healthcare, expects this attack to cost them **$1.6 billion**. That amount does not include the ransom that UnitedHealth paid, estimated to be $22 million. UnitedHealth reported **$872 million** in unfavorable effects from this attack in its Q1 earnings report. Cyberattack impacts in that quarter resolved at **$0.74 per share**, with the company estimating full-year impacts of $1.15 to $1.35 per share.

UnitedHealth said they provided **an estimated $6 billion** in advance funding and interest-free loans to impacted care providers. However, this was still a devastating blow for some medical centers and physicians' offices. According to an **American Medical Association (AMA) survey** of the practices and clinics impacted by this cyberattack, the incident had a cascade of damaging effects on medical offices. The AMA reported that 31% of their survey respondents were unable to make payroll, 55% of respondents had to use personal funds to cover practice expenses and 44% were unable to purchase supplies.

TREND 2: RANSOMWARE THAT DISRUPTS PUBLIC SERVICES

VICTIM:
The City of Hamilton, Canada

FIRST REPORTED:
The Week in Breach News: 03/06/24 – 03/12/24

EXPLOIT:
Ransomware

Our initial report: The City of Hamilton, Canada, a municipality located about 40 miles away from Toronto, experienced a ransomware attack that impacted city systems and services. The attack was discovered on February 25. Critical infrastructure, including water and wastewater treatment, waste collection and transit are operational but many other city services are not. Citizens must pay taxes, tickets or fines in person. Most public agencies are without phone service, and libraries are unable to offer Wi-Fi. All city council meetings before March 15 have been canceled. No ransomware gang has claimed responsibility for the attack.

The aftermath: Officials said that **about 60%** of the municipality's roughly 700 servers were encrypted. Systems used for online payments were knocked out, forcing the city to turn to cash transactions and other manual methods. Any tax payments, tickets or fines had to be paid in person. City workers did not receive pay stubs or pay reports, with some pay running two weeks late. As of April 16, 2024, many city government departments were still limping along, with no phones or access to systems and data, including accounts payable, building & planning, housing cemeteries, engineering services, forestry horticulture, job postings and recruitment, licensing and online city services.

TREND 3: DESTRUCTIVE ATTACKS ON MANUFACTURERS

VICTIM:
Varta AG: Battery manufacturer

FIRST REPORTED:
The Week in Breach News: 02/14/24 – 02/20/24

EXPLOIT:
Hacking

Our initial report: Varta AG announced that it was hit by a cyberattack that forced it to shut down IT systems and stop production at its plants. Varta AG said that its administration and five of its production units were taken down by hackers. The company did not provide a timeline for the restoration of its operations. The resultant production stoppage has caused a slide in Varta AG's stock price. Varta AG is a major battery supplier to automotive companies and countries throughout the EU.

The aftermath: Production was halted for at least two weeks, leading to a cascade of bad news. However, the company's production lines were moving as expected about a month after the attack. While Varta AG was already under a restructuring plan, the company cited the cyberattack as a major contributor to the fiscal woes that resulted in it being unable to meet its targets under the plan. **Shares fell by 30%** after the April 12, 2024 announcement.

TREND 4: NATION-STATE HACKERS SEARCHING FOR SPECIFIC INTELLIGENCE

VICTIM:
Microsoft

FIRST REPORTED:
The Week in Breach News: 01/17/24 – 01/23/24

EXPLOIT:
Password spraying

Our initial report: Microsoft disclosed that several of its corporate email accounts were breached by a Russian state-sponsored hacking group Midnight Blizzard. The company detected the attack on January 12, 2024. Microsoft's internal investigation concluded that the attack was conducted by a group of Russian threat actors associated with Nobelium/APT29 (sometimes known as Midnight Blizzard or Cozy Bear). The software titan said that the threat actors breached their systems in November 2023 by conducting a password spray attack to access a legacy non-production test tenant account. Microsoft said the hackers accessed a "small percentage" of Microsoft's corporate email accounts for over a month, including accounts tied to the company's leadership team and employees in the cybersecurity and legal departments. The company speculates that the threat actors were looking for information about their own gang.

The aftermath: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a rare binding emergency directive **on April 2, 2024**, to an undisclosed number of federal agencies, requiring them to change any logins that were affected and to investigate what else might be at risk. Officials are concerned that the suspected Russia-aligned hackers obtained passwords and other secret material that might allow them to breach multiple U.S. agencies. Agencies have until April 30 to complete CISA's directive and provide weekly updates on the progress made to reset passwords, session tokens and other authentication tools. CISA said that by September 1, 2024, it will provide a report to the heads of the Department of Homeland Security (DHS), the Office of Management and Budget (OMB) and the Office of the National Cyber Director (ONCD) on any outstanding issues related to the hack.

TREND 5: ZERO-DAY EXPLOIT PRESSURE RISES

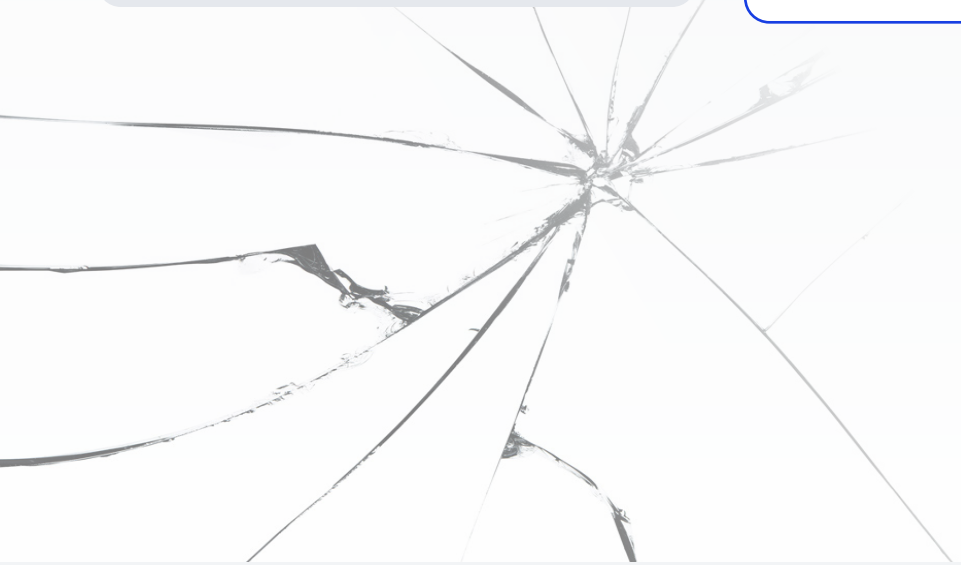
VICTIM:
Xfinity

FIRST REPORTED:
Link

EXPLOIT:
Zero-day

Our initial report: Xfinity announced that it experienced a data breach in late October 2023 because of the Citrix Bleed vulnerability. The company said that hackers breached one of its servers and obtained customer information, resulting in data exposure for an estimated 35.9 million people. The stolen data includes usernames and hashed passwords as well as customer names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. The Citrix Bleed vulnerability first surfaced in August 2023.

The aftermath: Rep. Ruben Gallego (AZ-03) sent a letter to Social Security Administration (SSA) Commissioner Martin O'Malley and Federal Trade Commission (FTC) Chair Lina Khan about the incident after learning that the incident may have exposed the Social Security numbers of **an estimated 65,000 Arizonans**. He also asked the FTC to recommend further legislative actions that would ensure consumers are better protected in situations like this one. At least three federal suits have been filed in Florida's Southern District court and several class action lawsuits were filed as well, including one in Pennsylvania and three in Florida.



TREND 6: RANSOMWARE ASSAULTS IN THE EDUCATION SECTOR DISRUPT LEARNING

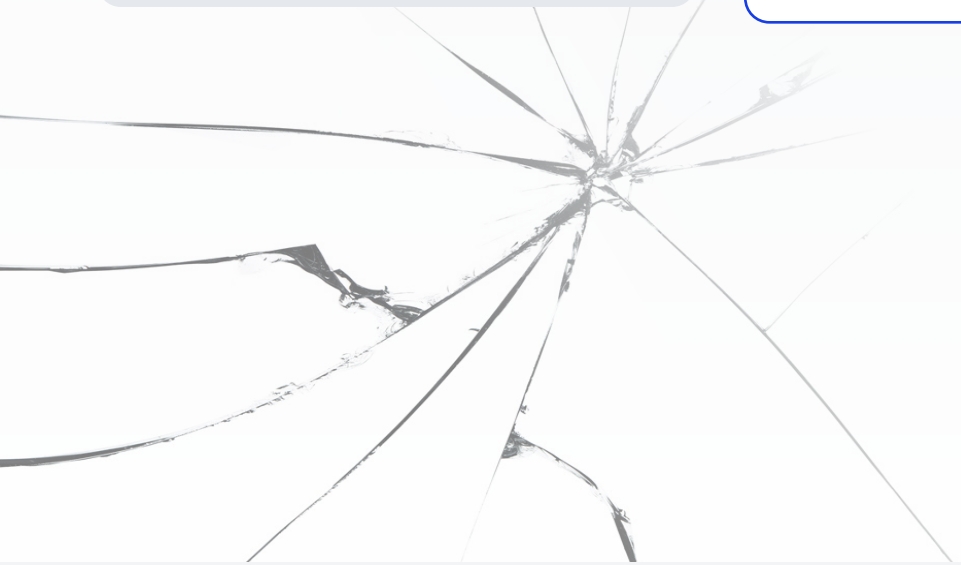
VICTIM:
Scranton School District (Pennsylvania)

FIRST REPORTED:
The Week in Breach News: 03/13/24 – 03/19/24

EXPLOIT:
Ransomware

Our initial report: Schools in Pennsylvania's Scranton School District were impacted by a cyberattack in March 2024. The district said on social media that it is experiencing widespread technology outages because of the attack. Students in many areas have been unable to connect to school networks and forced to resort to old-fashioned paper and pencil. School officials also noted that some files are unavailable. The district is investigating the incident with a third-party forensics firm.

The aftermath: On the day the attack initially hit, schools in the district were delayed in opening. Subsequently, schools opened but technology problems continued to interrupt and hamper school operations. Faculty and staff were left with no access to student records, email or phone systems. In the classroom, teachers and students were forced to resort to old-fashioned paper and pencil learning after the attack left them unable to use computers. These delays continued for over a week, with school district officials unable to offer a timeline on when the full functionality of the school's technology would be restored.



TREND 7: HACKERS TRYING TO SQUEEZE CASH OUT OF DATA EXPOSURE VICTIMS

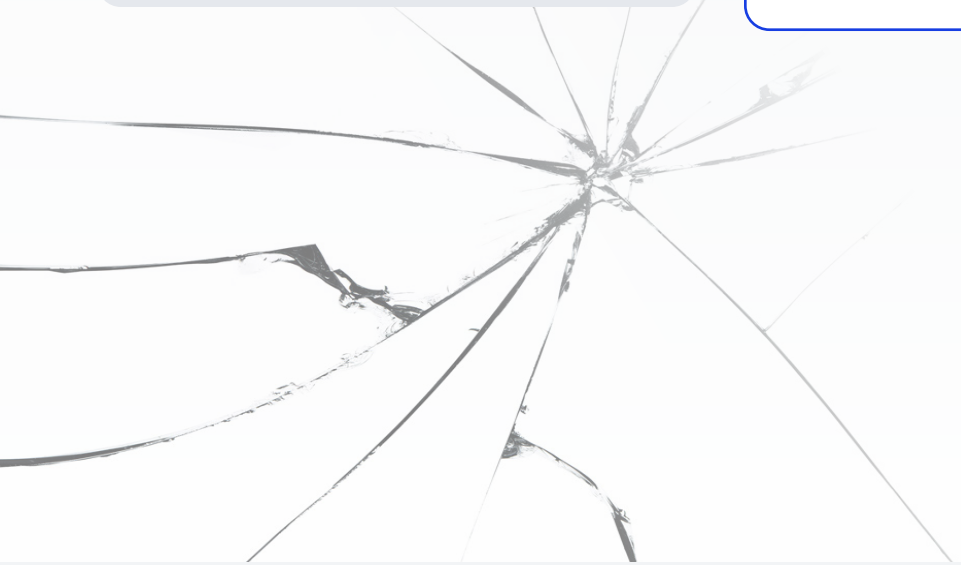
VICTIM:
MediaWorks

FIRST REPORTED:
The Week in Breach News: 03/20/24 – 03/26/24

EXPLOIT:
Hacking

Our initial report: A cyberattack on MediaWorks may have resulted in data exposure for an estimated 403,000 people. The company said that the attack took place on March 14. The perpetrator has been identified as OneERA, who claims they stole 2,461,180 records purportedly containing personally identifiable information (PII) of individuals in New Zealand. The attackers advertised the sale of MediaWorks' data, including PII and data from other sources like survey responses, videos, music content and electoral information. MediaWorks said that The Privacy Commissioner and police have been notified.

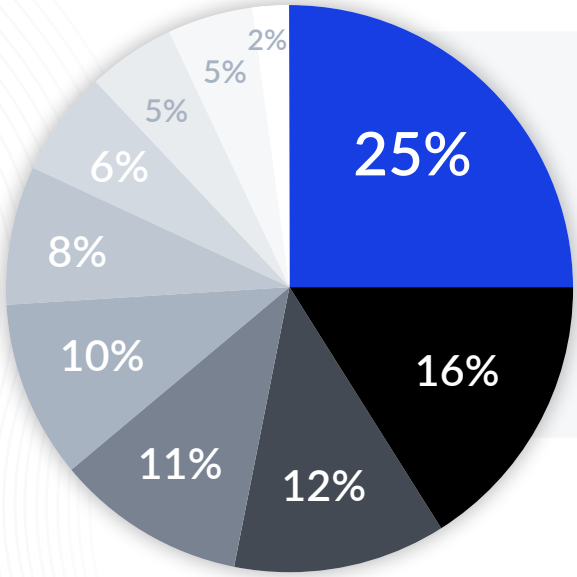
The aftermath: The hackers mounted an effort to extort the individuals who had their data exposed. Hackers contacted an undetermined number of the victims directly through email. In the messages, the cybercriminals told the victims that MediaWorks was unwilling to negotiate with them, so they intended to publish the data. The hackers demanded **a ransom of $500** in cryptocurrency to not include their stolen personal data in the tranche. Eventually, the bad actors released the stolen data on the dark web.



LOOKING AHEAD TO FUTURE TROUBLE

When thinking about how their organization could be at risk of a cyberattack, a quarter of the people we talked to for the Kaseya Security Survey 2023 pointed to email. This really shows how crucial it is to have strong, multilayered email security measures to keep risks low. Another quarter said that their organization's biggest weak spot is endpoint security (23%). Interestingly, 22% feel that human factors, like mistakes or insider threats, are the likeliest paths for a cyberattack on their company. This underlines just how vital it is for every employee to go through security training and to have a security operations center (SOC) ready to respond if an incident does happen. A well-educated workforce can significantly lower the chances of a cybersecurity incident.

WHICH OF THE FOLLOWING THREAT VECTORS ARE YOU MOST CONCERNED ABOUT BEING THE GATEWAY TO A SUCCESSFUL ATTACK IN THE NEXT 12 MONTHS?



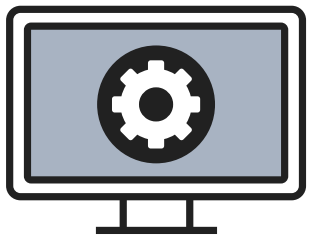
- *Email*
- *Human error (social engineering, distraction)*
- *Endpoint (server)*
- *Endpoint (laptop)*
- *Cloud*
- *Network*
- *Insider threats*
- *Supply chain*
- *Unpatched systems (zero-day attacks)*
- *None*

78% of IT professionals believe their organization will be hit by phishing in 2024 .

10 SMART SECURITY MOVES TO MAKE RIGHT NOW

Cybersecurity will continue to remain turbulent in 2024, with twists and turns that no one expects. Businesses need to act now to increase their cyber resilience and fortify their defenses. These tips can help ensure they're making all the right moves.

- **Conduct regular, comprehensive security awareness training.**
- **Frequently train employees with phishing simulations.**
- **Get a clear picture of dark web data risks.**
- **Regularly run penetration tests to learn how cybercriminals can penetrate defenses.**
- **Implement smart email security that can intercept and eliminate malicious emails automatically.**
- **Don't neglect maintenance. Patch software and systems regularly.**
- **Consider choosing a managed security operations center (SOC) to have heavy-duty cybersecurity expertise available at all times.**
- **Invest in endpoint detection and response (EDR) technology to speed up incident response.**
- **Create, update and drill incident response plans, including plans for cyberattack-specific scenarios like ransomware.**
- **Assess the cyber resilience of vendors and service providers.**



KASEYA'S SECURITY SUITE CAN HELP BUSINESSES STEER CLEAR OF CYBER TROUBLE IN 2024 AND BEYOND

BullPhish ID

Our effective automated security awareness training and phishing simulation solution provides critical training that improves compliance, prevents employee mistakes and reduces a company's risk of being hit by a cyberattack.

Dark Web ID

Our award-winning dark web monitoring solution is the channel leader for a good reason: it provides the greatest amount of protection around with 24/7/365 human and machine-powered monitoring of business and personal credentials, including domains, IP addresses and email addresses.

Graphus

Our automated email security is a cutting-edge solution that puts three layers of AI-powered protection between employees and phishing messages. It works equally well as a standalone email security solution or supercharges your Microsoft 365 and Google Workspace email security.

RocketCyber Managed SOC

Our managed cybersecurity detection and response solution is backed by a world-class security operations center that detects malicious and suspicious activity across three critical attack vectors: endpoint, network and cloud.

LEARN MORE ABOUT OUR SOLUTIONS!

SECURITY
SUITE

Kaseya