SENDMARC

2024 Cyberthreat Report

Exploring the state of email security & DMARC

What's inside

Introduction

Email has been around for almost **six decades**[1] and during that time, it has become a vital communication channel and powerful marketing tool for businesses worldwide. But businesses aren't the only ones taking advantage of email's popularity. Cybercriminals leverage vulnerabilities in email security to launch malicious attacks at an ever-increasing rate with 2023 seeing some of the largest attack statistics to date.

A critical challenge in today's digital age is that technological innovation is advancing at a pace security teams are struggling to match. In addition to the advancements in existing threats, the rise of generative artificial intelligence (AI) has ushered in a new era of sophisticated cyberattacks that threaten to devastate businesses.

These factors combined with a widening cybersecurity skills gap, make cyber risks increasingly pronounced. IT teams remain stretched with **50% of businesses**[2] that experienced a breach last year saying they're understaffed.

Threats continue to cause immense business damage, with cybercrime expected to cost the world over $23 trillion[3] annually by 2027.

Considering that the majority of cyberattacks begin with an email, businesses need to take the security of their email ecosystems systems seriously. The nature of cyberattacks looked at in our research reveal that email security isn't only about protecting your organization's stakeholders but is critical to shielding your brand's reputation and continuity.

This report explores:

1. **Email usage and risks in modern business**
2. **Top threats to your business**
3. **Best practices for email security**
4. **The state of DMARC and its critical role in protection**

Key findings

An average of over
361 billion emails
are sent daily

91%

91% of all cybercrimes
start with an email

94%

Over 94% of businesses reported
email security incidents
in 2023

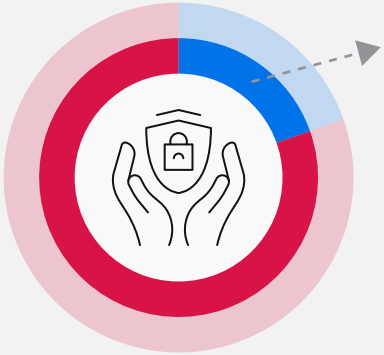
93%

93% of security leaders
expect to face
AI-driven attacks daily
in 2024

Business Email
Compromise (BEC) totaled
$2.9 billion in losses
in 2023

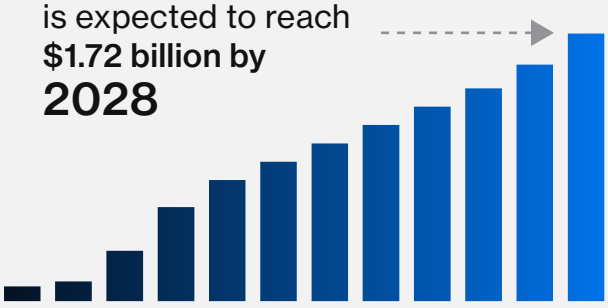
A ransomware attack is
expected to happen
every two seconds
by 2031

2023 was the worst year for
phishing on record with almost
five million attacks observed



Only **19.6%** of
email domains globally are fully protected
against
email-based
threats with
DMARC

The DMARC market size
is expected to reach
$1.72 billion by
2028



Email's dual faces

Essential tool & security risk

In today's digital world, where everyone's using social media, instant messaging apps, and digital collaboration platforms, email might seem outdated. But in reality, it remains an essential communication and marketing tool for businesses worldwide, with an average of over **361 billion emails**[4] sent globally every day.

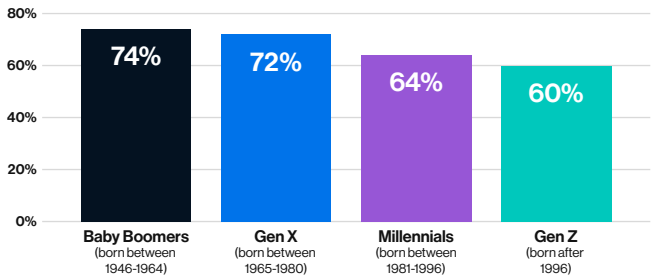
Businesses rely on email for daily internal communications and sending important updates, notifications, and reminders to clients and partners. In addition, with **4.5 billion users**[5] globally, email still offers a massive consumer audience to businesses, as highlighted by the **81% of companies**[6] still using email as part of their marketing strategies.

Email's popularity with marketers continues for various reasons: it's cost-effective (**ROI is currently $36 for every $1 spent**[7]), offers opportunities for personalization, and provides detailed analytics and tracking that make it easy for marketers to monitor its performance.

So, what do consumers have to say?

Email is still important to consumers too. **99% of them say they check their inboxes**[8] at least once a day, while others check email up to 20 times daily! Consumers across generations also consider email the **most personal**[9] way to get communications from a brand.

Percentage of people who believe email is the most personal brand communication channel:



The email flaw

There's a security flaw in email that makes it seriously vulnerable to cyberthreats, with **91% of all cybercrimes**[10] starting with an email. Given its widespread use, it's no wonder that email has also become a favorite attack method for cybercriminals looking to steal data, money, or both.

Your modern business is at risk of various email-based threats that continue to advance in strength and sophistication. This trend calls for your email security to do the same to protect your organization, staff, partners, and customers from the potential devastation of a successful cyberattack.

Speaking of cyberattacks, you may be wondering about the top email threats to watch out for in 2024. Read on to discover what these are.

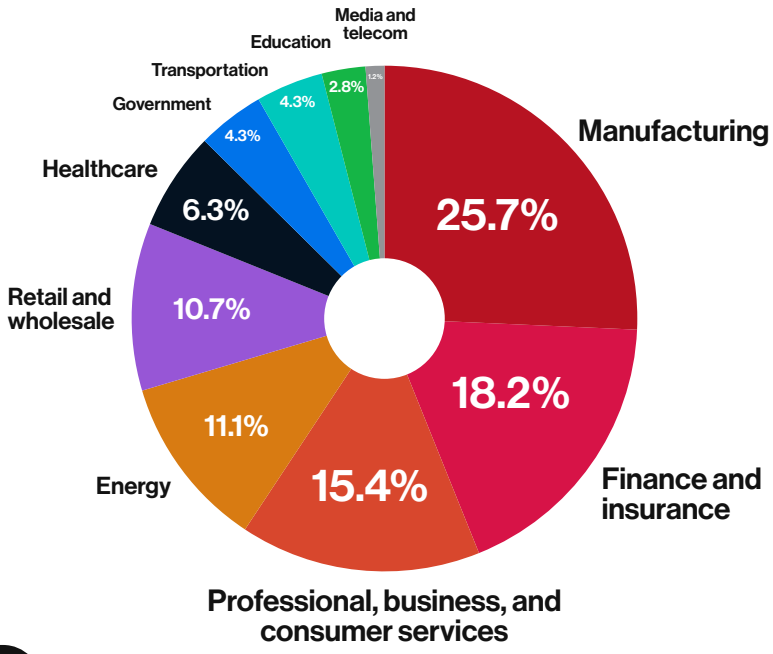
Assessing vulnerabilities:

Top threats to your business's email security in 2024

Over 94% of businesses[11] reported email security incidents last year; a big reminder that no business, large or small, is safe from being targeted by cybercriminals.

The top industries that experienced the **most cyberattacks[12]** globally in 2023 were:

- **#1** Manufacturing
- **#2** Finance and insurance
- **#3** Professional, business, and consumer services.



Contributing to the rise in companies' cybersecurity concerns are the expanding attack surfaces due to remote working and generative AI, alongside the previously mentioned growing tech skills gap that prevents organizations from adapting quickly enough to secure themselves.

Next, we explore some of the top email security threats to your business in the current digital landscape.

Top threats

1 Phishing

There are various forms of email phishing, including spear phishing, which targets specific individuals, and whaling, which targets senior or high-profile employees, to name a few.

This tactic involves a cybercriminal impersonating a trusted sender – like your business or staff – to deceive email recipients into revealing sensitive information like login credentials, financial information, or other personal data.

Another favorite phishing tactic is where cybercrooks intercept and change banking details in payment requests or invoices to redirect payments to their own accounts.

Phishing remains a top attack method for cybercriminals in the current digital landscape and is the entry point for many other types of attacks including ransomware and malware.

Last year was the worst year for phishing on record[13], with the Anti-Phishing Working Group observing almost five million phishing attacks.

In March 2024, Trustwave SpiderLabs uncovered a **phishing campaign[14]** that was using emails disguised as bank payment notices to distribute Agent Tesla, an info stealer and keylogger. The emails prompted recipients to open an attachment that concealed a malicious loader that deployed Agent Tesla on the host system, enabling it to escape detection. This is just one sneaky way cybercriminals trick users into compromising their systems and data.

As these attacks continue to advance, it's becoming more difficult for even the most tech-savvy users to spot them, with **nearly 300 thousand[15]** falling victim to phishing attacks in the U.S. alone in 2023. With approximately **3.4 billion phishing emails[16]** being sent every day, phishers show no signs of slowing down.

Top threats

2 Generative AI

Generative AI is a type of AI that uses prompts to create copy, visuals, videos, and other data using generative models, like **ChatGPT[17]**, Copilot, and Gemini, for example.

Cybercriminal abuse of AI tools led to a massive rise in the complexity and intensity of cyberattacks like social engineering and ransomware attacks last year. These types of attacks are set to increase, with 93% of security leaders[18] expecting to face AI-driven attacks daily in 2024.

Malicious users are training AI models to create code that, if deployed, can be exploited for attacks. Security experts also **highlight privacy risks[19]** associated with using large language models (LLMs). If proprietary or personal information is entered into free versions of these models, it's considered a breach because this data can be used to train LLMs and is accessible to other users.

Cybercriminals are misusing generative AI to produce increasingly convincing cyberattacks[20] at scale.

The use of AI in businesses has **almost doubled[21]** in the last year, but organizations' security measures aren't advancing with this adoption with just **24% of generative AI[22]** measures in businesses being secured. This is a huge worry because it leaves many businesses vulnerable to rising AI-related security threats.

IBM states that this insufficient security will lead to breaches, potentially reducing the benefits that generative AI projects are intended to deliver to businesses – a prediction that's already coming true, with **77% of companies[23]** having experienced breaches in their AI systems in the past year.

Experts believe cybercrooks will continue to ramp up their attacks using generative AI to help them create even more convincing phishing emails and deepfakes, crack passwords, and impersonate businesses.

Top threats

3 Social engineering

Social engineering is a tactic cybercriminals use to manipulate people into giving them confidential information, often leading to unauthorized access to data or systems. This type of attack relies on human error and usually plays on emotions like fear, trust, or empathy to trick people into making security mistakes, posing serious threats to organizations.

Social engineering attacks are becoming more sophisticated and detailed, making it harder for employees to recognize fake emails and websites. Their reliance on manipulating individuals continues to pay off, as highlighted by the 95% of security breaches[24] caused by human error.

In the **largest known social engineering attack ever[25]**, a cybercriminal tricked Google and Facebook employees into sending over $100 million to fake company accounts he'd set up. He posed as a legitimate computer manufacturer that did business with both companies and sent phishing emails with invoices for real services, redirecting payments to his fraudulent accounts.

In 2024, these scams only seem to be gaining cybercriminal favor with social engineering techniques being used in a staggering 98% of cyberattacks[26].

Top threats

4 BEC

Business Email Compromise (BEC) is an advanced scam in which cybercriminals trick a company, its employees, customers, or partners into sending them money or sensitive data. Types of BEC attacks include phishing, spoofing, and impersonation, to name a few.

Like many others, BEC attacks have become increasingly sophisticated in recent years, with criminals doing detailed research to effectively imitate internal communications as well as brand style and tone.

For example, they've exploited hacked emails to ask for wire transfers, pretending these are for critical and confidential business transactions. Often, these deceptive emails are only recognized as fraudulent after the money has been sent, resulting in significant financial damage to businesses.

70% of organizations[27] have been the targets of BEC attacks within the last year.

The growth in BEC attacks is having a huge financial impact on companies of all sizes. In 2023, the FBI's Internet Crime Complaint Center (IC3) got almost **21 500 complaints of BEC[28]**, which totaled losses reaching $2.9 billion.

Top threats

5 Data breach

A data breach is a security incident in which an attacker gains access to sensitive, confidential, or protected information. Hackers use several techniques to achieve this including phishing, malware, or ransomware to invade systems and steal data.

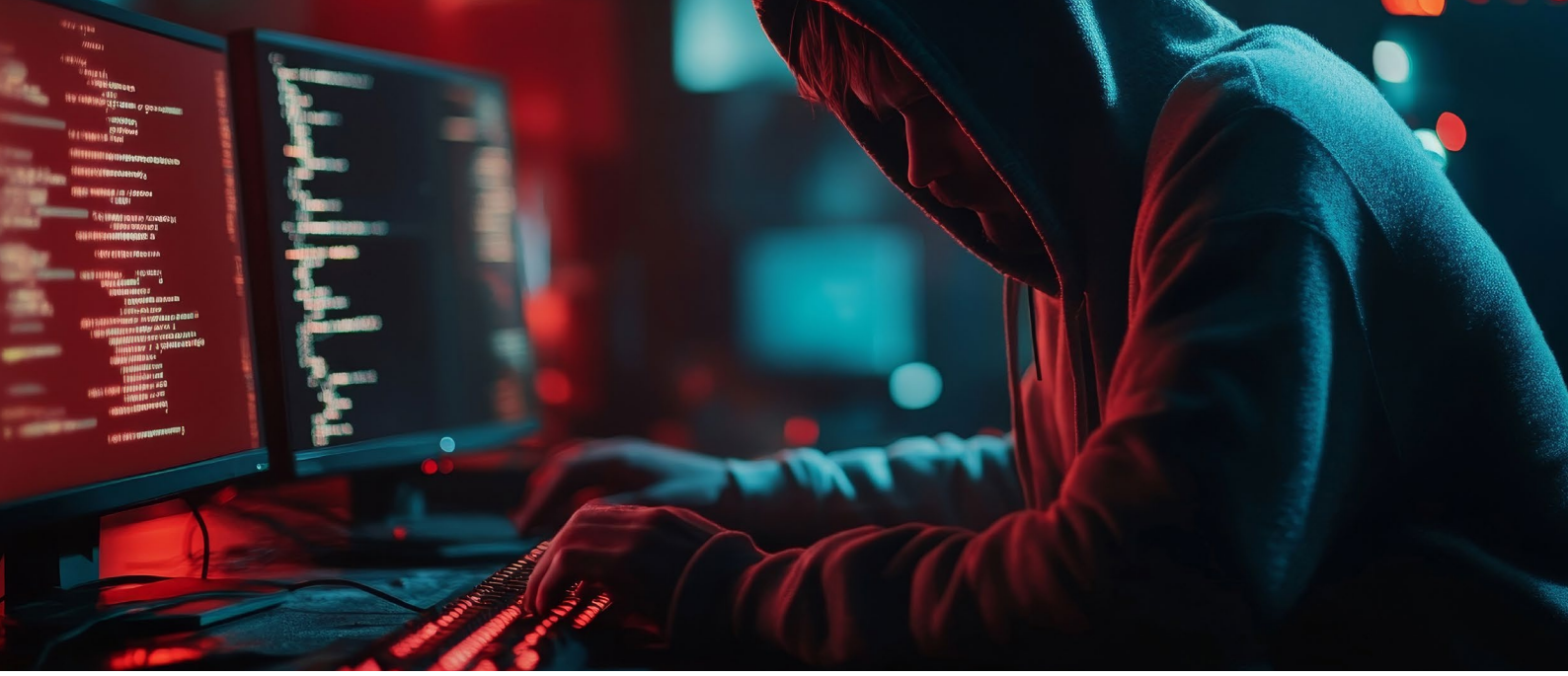
Within the first half of 2024, almost 36 billion records were[29] breached in 9478 publicly disclosed incidents with IT services and software, and healthcare, being the most-targeted industries.

The global average cost of a data breach soared to **$4.88 million in 2023[30]**, a 10% increase over 2022 and the highest spike since the COVID-19 pandemic. The rise in costs was mostly due to expenses related to business disruption and post-breach responses.

According to IBM, a staggering 70% of organizations[31] said they'd experienced significant or very significant business disruption resulting from a breach this year.

The type of data most often stolen or compromised in breaches in the last year included employee personally identifiable information (PII), customer PII, intellectual property, other corporate data, and anonymized customer data (non-PII).

2023 saw a **72% increase in data breaches[32]** since 2021, a trend that underscores the persistent and expanding threat of data breaches in our digital age.



Top threats

6 Ransomware

Ransomware is a type of attack that blocks the victim's access to a computer system or data until a ransom is paid. These attacks can bring critical systems to a standstill and result in large payouts.

The price of ransomware attacks soared by 140% last year, costing victims a staggering $1.1 billion[33]. According to Statista, the number of ransomware attacks in 2023 marked a new peak in global ransomware activity, setting a record for the highest payments seen since the COVID-19 pandemic.

By 2031, a ransomware attack is expected to happen every two seconds[34] and by that same year, these attacks are predicted to cost global victims over $265 billion[35] in damages.

No business large or small is safe with 72.7% of organizations[36] falling victim to a ransomware attack in 2023. In the current landscape, the World Economic Forum (WEF) says ransomware gangs are using more ruthless tactics[37] and targeting more vulnerable victims, including hospitals.

One attack in June this year hit London hospitals[38], causing the re-arrangement of 800 planned operations and 700 outpatient appointments, including five C-sections and 18 organ transplants. The NHS England, London, had to declare a regional incident and rely on neighboring providers and national partners to cover affected services.

The trend unfortunately isn't positive, and ransomware has been called 'more brutal' than ever in 2024[39]. It's expected that attackers will continue to go after the most vulnerable organizations in pursuit of their paydays.

Top threats

7 Malware

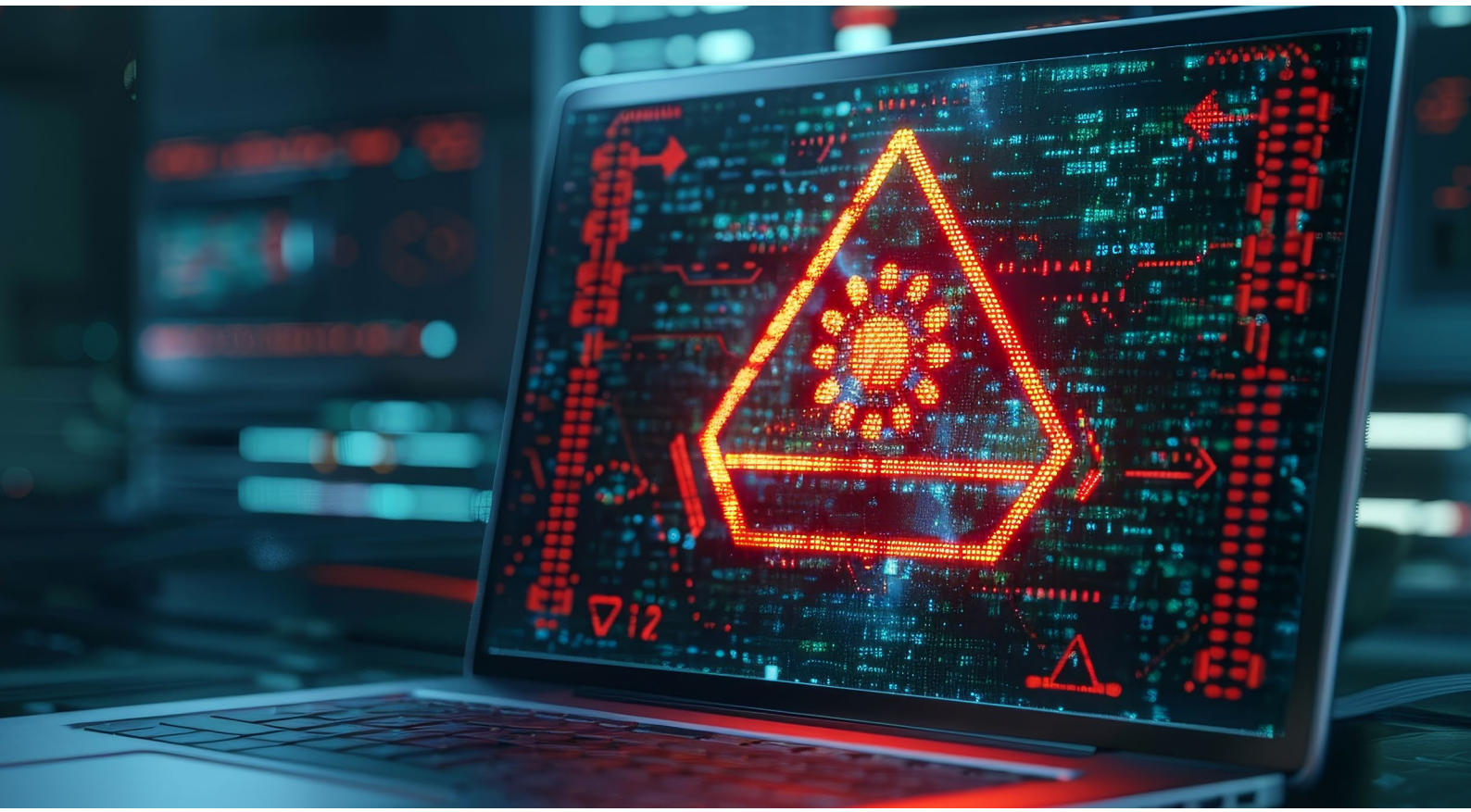
Malware is malicious software that can include spyware, keyloggers, ransomware, and trojans, often delivered by what seem like harmless links or attachments. Once downloaded, malware can provide cybercriminals access to not only the victim's computer but the entire network within an organization. It can disrupt operations, steal information, and cause harm in many other ways.

> **Every day, 560 thousand new pieces of malware[40] are detected. This attack method remains a critical concern for organizations worldwide with experts predicting that the frequency of these attacks will only increase in the future.**

There were **over 6 billion malware attacks[41]** in 2023 with phishing being a **leading cause[42]** of infections. This is another type of threat that counts on human error to be successful – like social engineering - and these numbers show that it's still a successful method for cybercriminals.

In a **massive malware attack[43]** this year, the FBI dismantled a network of 19 million malware-infected computers across 200 countries that were thought to comprise the world's largest botnet. Access to this network was sold and enabled crimes, including billions of dollars of financial fraud and identity theft.

Cybercriminals select their victims based on their vulnerability and the amount of valuable data they hold. The **most attacked industries[44]** include manufacturing, finance, professional services, and healthcare, but education became the new big target in 2023. In addition, malware incidents targeting insurance firms experienced the sharpest increase across all sectors.



Top threats

8 Tech skills shortage

Around the world, organizations are experiencing a shortage of tech professionals and skills needed to protect themselves in the current threat landscape.

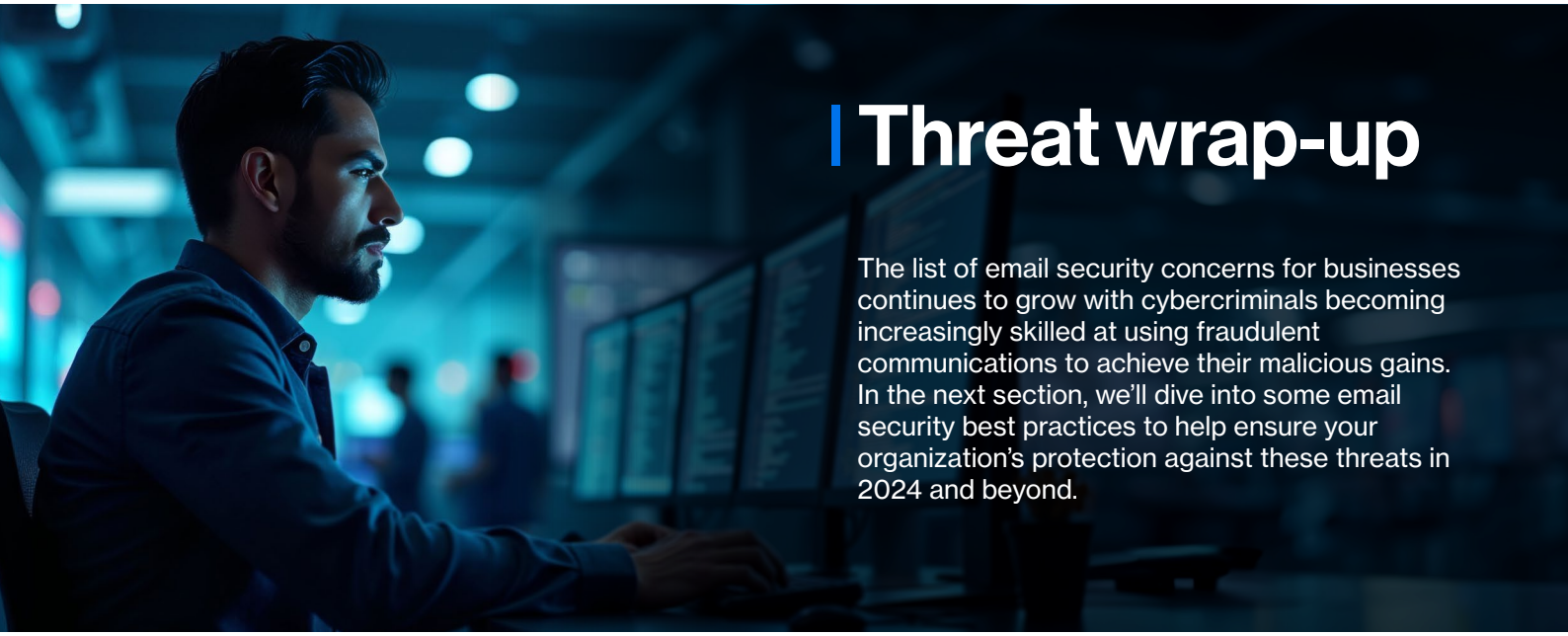
An expanding IT skills shortage is preventing businesses from finishing digitization projects and adopting new technologies - including AI – ultimately, impacting bottom lines.

A recent IDC Research survey revealed that nearly two-thirds of over **800 North American IT leaders**[45] reported insufficient skills leading to missed revenue targets, quality issues, and decreased customer satisfaction.

Within the next two years, it's predicted that 90% of organizations[46] **will suffer a critical tech skills shortage and by 2030 the world could see a shortage of 4.3 million tech workers**[47]**.**

This is a serious problem for businesses, with IBM reporting that **half of breached organizations**[48] in 2023 had severe staffing shortages, a skills gap that increased by double digits from 2022. This shortage resulted in an average of $1.76 million more in breach costs.

In a recent survey by the WEF, **78% of people**[49] said that their organizations don't have the required in-house skills to fully achieve their cybersecurity goals. The training and hiring needed to close this gap isn't keeping up with advancements in cyberthreats and though **one in five businesses**[50] use generative AI security tools to boost productivity and efficiency, this skills gap remains a challenge.



Threat wrap-up

The list of email security concerns for businesses continues to grow with cybercriminals becoming increasingly skilled at using fraudulent communications to achieve their malicious gains. In the next section, we'll dive into some email security best practices to help ensure your organization's protection against these threats in 2024 and beyond.

Expert's point of view on modern cyberthreats

Cybercriminals are getting more confident in their tactics for email-based hacking and BEC seems to top the chart when it comes to email-based threats. Executives are forever falling for these scams and clicking on links that lead to full compromise.

It's clear that most systems aren't able to detect these attacks, as even with 2-step verification in place, phishing emails slip through easily. Cybercriminals are doing better research and are using AI tools to craft the perfect emails, impersonating the right person, before sending out their phishing emails. This is making email-based attacks more successful by the day.

Dr Bright Gameli Mawudor, PhD

Cybersecurity Thought Leader

Public Speaker

Advisory Board Member

Mentor

Top 40 under 40 2026/2021 Tribe of Hackers: BlueTeam 2020

https://www.linkedin.com/in/bright-gameli-mawudor-phd-4324b238/

Email security in 2024 & beyond:

Best practices for business protection

Cyberthreats are constantly evolving, which means that your business's email security should adapt to provide visibility of and protect against these new threats as they arise. By doing this, you ensure that your organization is safe from the potential damages of a cyberattack. Read on to explore some best practices to ensure the safety of your email communications.

Best practices for business protection

Use strong passwords & MFA

Implement strong password policies along with multi-factor authentication (MFA) to ensure that only authorized users can access your business's email accounts. The current recommendation from the National Institute of Standards and Technology (NIST) is to use lengthy – not complicated – passwords, e.g. suMmersKiesaRebeaUtiful. It's also vital not to re-use passwords across accounts.

Update software often

Keep your organization's email systems and client software updated to protect against the latest vulnerabilities that could be exploited by attackers. Keeping software updated is also a requirement for compliance with many data protection standards and regulations.

Educate & train users

It's vital to keep your employees updated on how to identify phishing and other malicious email threats, especially considering that most security breaches today are caused by human error. Hold regular training sessions and send phishing email tests to get an idea of how aware your staff are.

Implement AI usage policies

The race to leverage AI for improved efficiency across every industry and department is leading to privacy and security issues. To guard against these issues, your organization must have strict AI implementation and usage policies for employees. These could include things like which AI tools employees are allowed to use and what they may be used for, regulations on what data employees are allowed to put into AI tools and any regional laws around AI usage*.

*Get more information on crafting effective AI usage policies here:
www.techtarget.com/searchsecurity/tip/How-to-craft-a-generative-AI-security-policy-that-works.

Prioritize email authentication

Implement global best practices in email authentication like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), to help prevent brand spoofing and impersonation.

- ✓ **SPF:** Checks that an email's sender is who they say they are, and that they're authorized to send email from a domain.
- ✓ **DKIM:** Verifies that an email hasn't been intercepted or tampered with during transit.
- ✓ **DMARC:** Allows a domain owner to specify how email receivers should treat messages that claim to come from their domain but fail SPF and DKIM checks.

When configured correctly, SPF, DKIM, and DMARC prove that an email sender is legitimate and that the message hasn't been compromised, ensuring that only emails that've passed authentication checks reach an inbox.

Best practices wrap-up

All these best practices are crucial to your business's protection and continuity. It's important to note that there's been a magnified focus on email authentication, especially DMARC, in recent years, as experts have realized these protocols' critical role in the fight against fraudulent emails.

While anti-spam is excellent for blocking unwanted bulk emails, it isn't enough to secure your business against email-based cyberattacks. This is because even with anti-spam in place, cybercriminals can use your organization's domain to send malicious emails targeting your external stakeholders. DMARC steps in to solve this problem, ensuring that fraudulent emails aren't delivered to inboxes.

The problem is that DMARC adoption isn't happening fast enough, even with enterprises, governments, and regulators making its implementation mandatory, leaving many businesses vulnerable to email-based cyberattacks.

Dive deeper into the state of DMARC in the next section of this report.

Shielding businesses from cyberattack damage:

The state of DMARC in 2024

By implementing DMARC with the strongest policy (p=reject), and as long as the recipient server adheres to your DMARC policy, fraudulent emails are blocked, and won't reach the inboxes of staff, partners, customers, or any of your other stakeholders.

Rising email fraud – especially phishing - has pushed DMARC into the limelight in recent years as mandates for its implementation from email giants like Google and Yahoo, as well as governments and regulatory bodies, take effect around the globe. These mandates make one thing clear:

DMARC is no longer a nice-to-have, but a must-have for businesses.

In this section, we explore the current state of DMARC.

Current state of DMARC

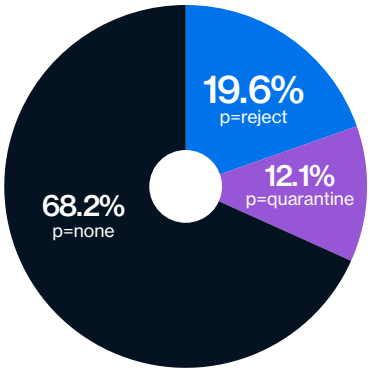
Mandatory DMARC implementation requirements continue to rise.

DMARC is now strongly recommended or required by:

Google & Yahoo	**PCI DSS 4.0**	**NIST**	**GDPR**
Email sender requirements	Payment Card Industry Data Security Standard	National Institute of Standards and Technology	General Data Protection Regulation
GLBA	**CMMC 1.0**	**HIPPA**	**CCPA**
The Gramm-Leach-Billey Act	Cybersecurity Maturity Model Certification	The Health Insurance Portability and Accountability Act	California Consumer Privacy Act

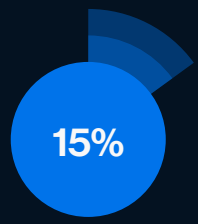
The number of valid **DMARC policies increased by** 84% in 2021

Less than 6 million **DMARC records** existed worldwide as of 2022



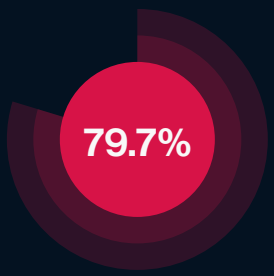
Only 19.6% of email domains are fully protected with a p=reject DMARC policy

P=none was the most common DMARC policy as of Q2 2022.



of **Fortune 500 companies actively use DMARC**

Compound Annual Growth Rate (CAGR) of the global DMARC market from 2024 - 2031



of domains **don't have DMARC**

$1.72 billion
Expected global **DMARC market size** by 2028

Sources:
https://sendmarc.com/google-yahoo-sender-authentication-requirements/
https://sendmarc.com/anti-phishing-spoofing-pci-requirements/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
https://gdpr-info.eu/
https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act
https://www.cmmc-eu.com/cmmc-framework/
https://www.hhs.gov/hipaa/index.html
https://oag.ca.gov/privacy/ccpa
https://sendmarc.com/the-rise-of-dmarc/
https://dmarc.org/stats/dmarc/
https://llcbuddy.com/data/dmarc-statistics/

Expert's point of view on modern cyberthreats

I've seen the power of DMARC first-hand, watching it take an organization with thousands of daily email spoofing attempts down to nearly zero.

It prevents the delivery of false emails but also deters the 'bad guys' from trying once they know it's a waste of time. Every organization, large or small, should implement DMARC to protect their brand, partners, and customers.

J. Peter Bruzzese

ClipTraining Co-Founder & Chief Content Officer

Host of Security Insights

Nine-time Awarded Microsoft MVP

Co-Founder of the Central Florida Microsoft 365 User Group

https://www.linkedin.com/in/j-peter-bruzzese-98b6474/

www.cliptraining.com

Overlooking email security:

A dangerous business mistake

Failing to prioritize email security and compliance can lead to extensive and possibly irreversible damages to your business. In today's digital age, having strong email security isn't only about protection, it's also about maintaining your company's positive public image and safeguarding its long-term success.

In this part of the report, we explore the potential business damages caused by overlooking email security.

Breaks in communication

A successful email-based cyberattack could significantly disrupt your business's email flow in several ways including email downtime due to compromised systems, the blacklisting of your domain, or loss of critical emails and attachments. A phishing or impersonation attack would lead to fraud and misinformation which means less reliable and trustworthy communications overall. Not having the correct security standards in place could also cause non-compliance and negatively affect your business's email delivery.

Financial losses

Cyberattacks can result in huge direct financial costs, including expenses related to incident response, data recovery, legal fees and regulatory fines. The indirect financial losses caused by a successful attack can last longer because the damage to your business's reputation and loss of customer trust leads to lost business opportunities. IBM found that the cost of a data breach reached a record high in 2023 due to factors like operational downtime, lost clients, and higher post-breach response costs like additional support staff and increased regulatory fines.

Reputational damage

Data breaches and other cyberattacks can lead to the exposure of sensitive customer information, financial data, or intellectual property. These types of attacks, especially those that involve impersonating your business or staff, decrease customer and partner trust and their willingness to do business with you, ultimately impacting your bottom line and destroying your good reputation.

Operational disruption

Cyberattacks can cause system downtime for investigation and recovery, supply chain disruptions, as well as unnecessary stress for employees leading to reduced productivity. A ransomware attack on your organization for example, could bring operations to a standstill, with a cybercriminal stealing sensitive customer or financial data or hijacking systems until you pay a ransom to re-gain access.

Regulatory compliance issues

Failure to comply with industry regulations can result in penalties and fines as well as contribute to reputational damage. For example, by not complying with the **latest bulk sender requirements**[51] for DMARC implementation, the emails you send to Gmail and Yahoo users will be rejected or land in Spam or Junk folders – making your brand appear less trustworthy. In other cases, like the **PCI DSS's rule**[52] requiring that businesses handling payments have anti-phishing technology in place, failure to comply could lead to the suspension of a business's permission to process card payments.

Ultimately, the cost of having the right email security measures in place – including SPF, DKIM and DMARC – is likely far less than the cost of the damages your business would sustain if a cyberattack were to be successful. In fact, implementing and maintaining DMARC very likely costs less than what your business spends on coffee a month!

Conclusion & future forecast:

DMARC's leading role in email security

Protecting your email ecosystem and in turn your employees, customers, partners, and all other stakeholders against email-based threats has never been more important. Especially considering how much your business likely depends on daily email communications.

From our report's findings we can be sure of one thing: DMARC is a lifeline for businesses facing a rising tide of cyberattacks. As existing threats continue to advance, and new risks emerge, our experts believe that more mandates for DMARC implementation will be released.

"The push for DMARC implementation and enforcement will continue, and DMARC will become a requirement for all senders who want to send email to customers who use major mailbox providers," says Keith Thompson, Co-Founder and Chief Technology Officer at Sendmarc.

"This expanded DMARC adoption will lead to increased sophistication of email threats with bad actors looking for ways into organizations' infrastructures to perform attacks from within. We'll also see an increase in other forms of brand impersonation attacks."

"DMARC and its associated technologies will need to evolve to allow for greater control over a business's email security with cross-protocol (like BIMI, MTA-STS, and DANE) synergies. Integrated email security platforms combining threat protection technologies are becoming increasingly important as a result," Thompson concludes.

These insights make it clear that adopting DMARC isn't just a preventative measure but a strategic investment in the future of your business's digital security. As cyberthreats evolve in complexity and frequency, DMARC offers a necessary shield for your email communications, protecting all stakeholders against malicious messages.

Being proactive about DMARC adoption positions your business at the forefront of cybersecurity practices, ensuring you remain compliant with industry standards and resilient against emerging threats by ensuring every email sent from your domain is the real thing.

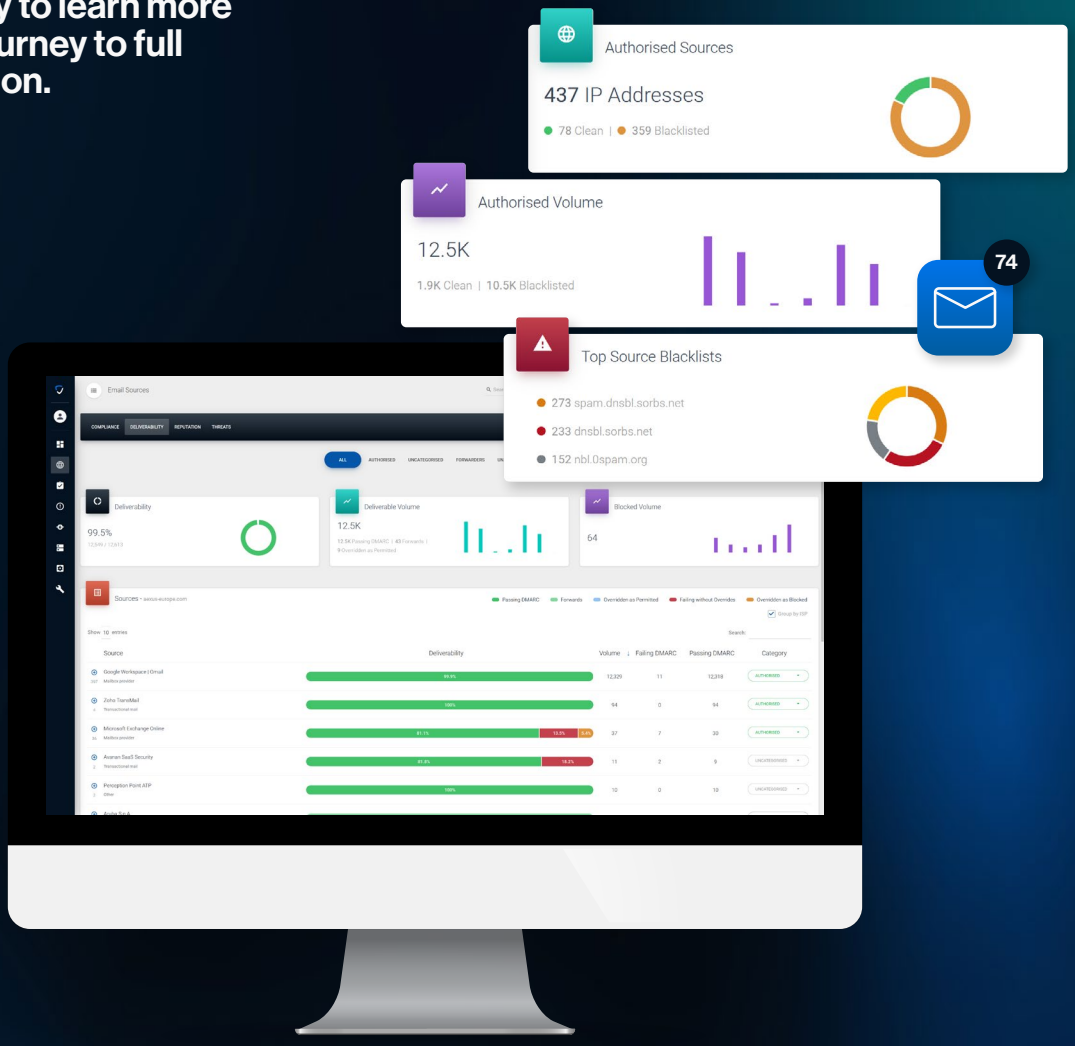
Secure your business with DMARC

In partnership with leading DMARC provider Sendmarc, we can help you protect your business against phishing, spoofing, and impersonation with automated and powerful DMARC, DKIM, and SPF control. Sendmarc's DMARC platform empowers the management of any number of domains and safeguards them against misuse and the sending of fraudulent emails.

DMARC with Sendmarc benefits:

- **Maximize deliverability**
- **Protect your brand**
- **Avoid financial implications**
- **Build customer trust**
- **Gain visibility through reports**
- **Comply with global standards**

Contact us today to learn more and start your journey to full DMARC protection.



Sources

Page 3

1. https://www.theguardian.com/technology/2002/mar/13/internetnews
2. https://www.ibm.com/reports/data-breach
3. https://www.state.gov/digital-press-briefing-with-anne-neuberger-deputy-national-security-advisor-for-cyber-and-emerging-technologies/

Page 5

4. https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/
5. https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/#:~:text=Global%20e%2Dmail%20audiences,daily%20e%2Dmails%20in%202025.
6. https://www.forbes.com/advisor/business/software/email-marketing-statistics/#:~:text=Email%20remains%20a%20powerful%20tool,potential%20as%20a%20marketing%20channel.
7. https://www.cognism.com/blog/email-marketing-statistics
8. https://www.cognism.com/blog/email-marketing-statistics
9. https://www.cognism.com/blog/email-marketing-statistics
10. https://sendmarc.com/the-growing-threat-of-email-phishing-scams-and-how-to-protect-your-business/

Page 6

11. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=In%202023%2C%2035%25%20of%20malware,for%20%242.7%20billion%20in%20losses.
12. https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Page 7

13. https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf
14. https://thehackernews.com/2024/03/alert-new-phishing-attack-delivers.html
15. https://www.statista.com/statistics/1390362/phishing-victim-number-us/
16. https://sendmarc.com/the-rise-of-dmarc/

Page 8

17. https://sendmarc.com/balancing-innovation-email-security-in-the-age-of-chatgpt/
18. https://www.helpnetsecurity.com/2024/04/29/offensive-ai-cyberattacks/
19. https://arcticwolf.com/resource/aw/the-state-of-cybersecurity-2024-trends-report
20. https://sendmarc.com/cybersecurity-redefined-adapting-your-businesses-strategy-to-combat-malicious-ai/
21. https://www.forbes.com/sites/chuckbrooks/2024/06/05/alarming-cybersecurity-stats-what-you-need-to-know-in-2024/
22. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/securing-generative-ai
23. https://www.helpnetsecurity.com/2024/04/25/cybersecurity-ai-stats/

Page 9

24. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/
25. https://www.tessian.com/blog/examples-of-social-engineering-attacks/
26. https://sprinto.com/blog/social-engineering-statistics/#:~:text=Social%20engineering%20scams%20are%20on,posing%20serious%20threats%20to%20organizations.

Page 10

27. https://arcticwolf.com/resource/aw/the-state-of-cybersecurity-2024-trends-report
28. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Page 11

29. https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024
30. https://www.ibm.com/reports/data-breach
31. https://www.ibm.com/reports/data-breach
32. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=In%202023%2C%2035%25%20of%20malware,for%20%242.7%20billion%20in%20losses

Page 12

33. https://www.statista.com/statistics/1410498/ransomware-revenue-annual/
34. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
35. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
36. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
37. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/
38. https://www.bbc.com/news/articles/cd11v377eywo
39. https://www.wired.com/story/state-of-ransomware-2024/

Page 13

40. https://www.getastra.com/blog/security-audit/malware-statistics/
41. https://www.statista.com/topics/8338/malware/#topicOverview
42. https://www.statista.com/statistics/1410445/cause-ransomware-attacks-global/
43. https://www.weforum.org/agenda/2024/06/botnet-cybercrime-zombie-computers/
44. https://www.statista.com/topics/8338/malware/#topicOverview

Page 14

45. https://www.idc.com/getdoc.jsp?containerId=prUS52128824
46. https://www.computerworld.com/article/2135542/within-two-years-90-of-organizations-will-suffer-a-critical-tech-skills-shortage.html
47. https://www.kornferry.com/content/dam/kornferry/docs/article-migration/FOWTalentCrunchFinal_Spring2018.pdf
48. https://www.ibm.com/reports/data-breach
49. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
50. https://www.ibm.com/reports/data-breach

Page 24

51. https://sendmarc.com/google-and-yahoo-tighten-email-authentication-standards-for-bulk-senders/
52. https://sendmarc.com/anti-phishing-spoofing-pci-requirements/