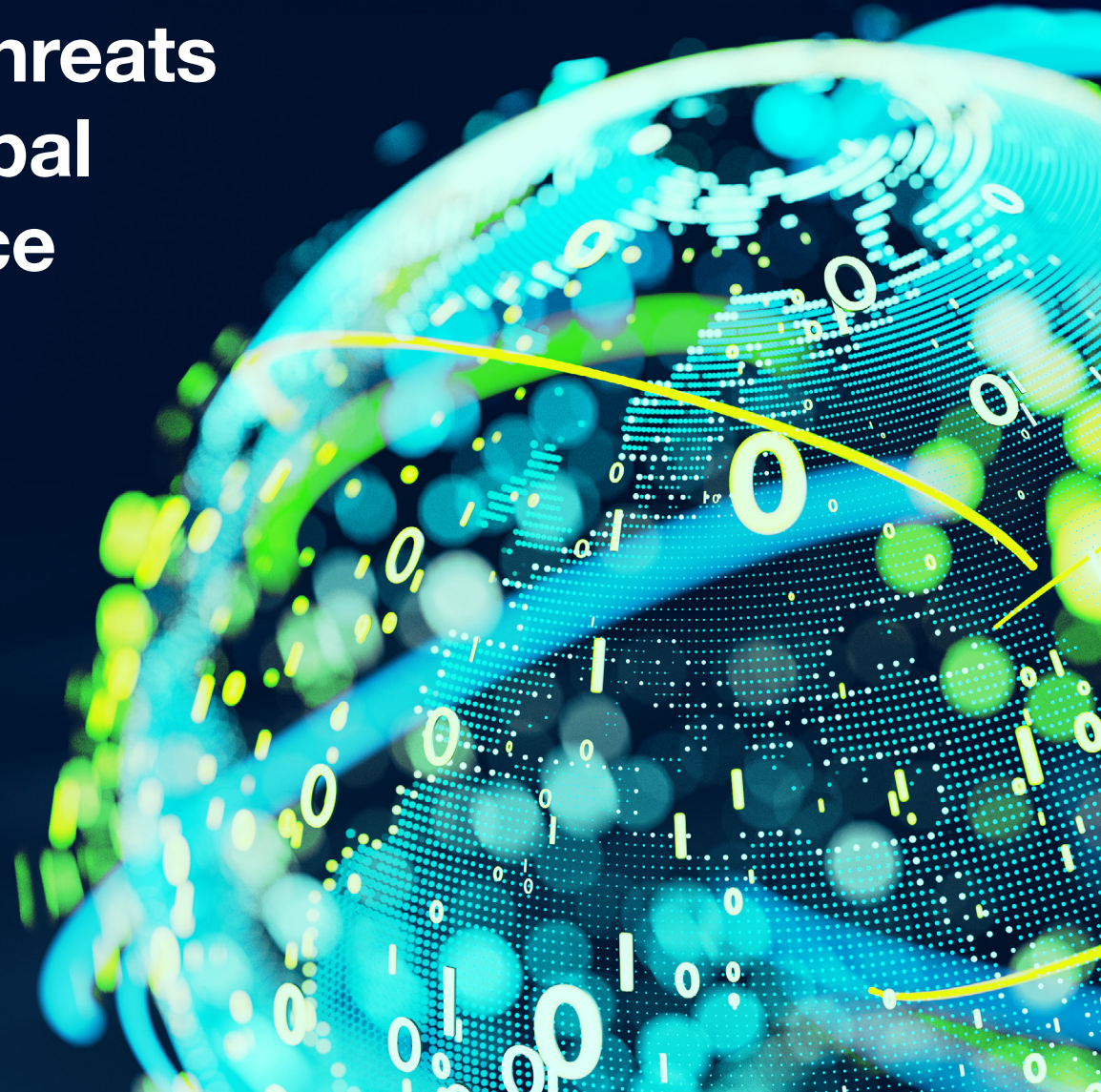




YUBICO COMPLIANCE EBOOK

# How modern cyber threats are transforming global regulatory compliance

The movement to Zero Trust and  
modern phishing-resistant authentication



# Contents

## **2 Table of contents**

## **3 Global compliance trends**

Data protection regulations by country

## **4 The evolving cyber threat landscape**

A glossary of evolving cyber attacks

## **7 Phishing-resistant authentication the foundation of emerging requirements**

What is phishing-resistant MFA?

What are passkeys?

Phishing-resistant MFA accelerates Zero Trust

The transition to ISO 27001:2022

## **11 The global compliance landscape**

National and state regulations

Consumer data privacy legislation

Cybersecurity legislation

Public sector & partners

Finance

Health & pharmaceuticals

Critical infrastructure sectors

## **26 YubiKey offers high-assurance, phishing-resistant MFA**

## **27 Takeaway**

## **28 A best practice checklist for security and compliance**

## **29 Sources**

## Snapshot from the 2024 report

### Global

- PCI DSS v4.0.1 new requirements effective March 31, 2025<sup>1</sup>



### North America

- 5 state privacy laws go into effect in 2024<sup>2</sup>
- OMB 22-09<sup>3</sup> and NSM-8<sup>4</sup> requirements for phishing-resistant MFA at AAL2 standards required by end of FY2024
- Revised NIST HIPAA guidance suggests MFA<sup>5</sup>



### Europe & the UK

- NIS2 Directive national laws across the EU enacted and applied after October 17, 2024<sup>6</sup>
- EU DORA requirements apply January 17, 2025<sup>7</sup>
- eIDAS 2.0 and European digital identity (eID) adopted in 2024, implementation by 2026<sup>8</sup>



### Asia Pacific

- India DPDP passed in 2023<sup>9</sup>
- Essential Eight Maturity Model is in effect in Australia<sup>10</sup>
- NISC Guidance is in effect Japan<sup>11</sup>

# Global compliance trends

A look at the evolving regulatory requirement for modern strong authentication

Across the globe, regulators and policymakers are responding to the cyber risk landscape by enacting or modifying laws to protect sensitive and critical data at the industry, state, country, and global levels. This scope of protection is also expanding, to include all the systems that process data (information technology) or manage operations (operational technology including industrial control systems) and to all the people (employees, third parties and customers), products and services that interact with the organization.

This report will examine the current global regulatory landscape for data security and privacy, the emerging focus on critical infrastructure sectors, and the regulatory shift to Zero Trust and modern strong authentication.

## Data protection regulations by country



This information in this report is intended for information only. The information may imperfectly represent global data protection laws or industry regulations and is not intended to comprehensively detail specific requirements.

## The evolving cyber attack landscape

Across the globe, regulators and policymakers are responding to the cyber risk landscape by enacting or modifying laws to protect sensitive and critical data at the industry, state, country, and global levels. This scope of protection is also expanding, to include all the systems that process data (information technology) or manage operations (operational technology including industrial control systems) and to all the people (employees, third parties and customers), products and services that interact with the organization.



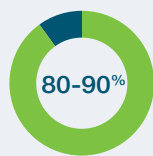
**\$4.88M USD**

global average cost of data breach<sup>12</sup>



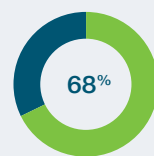
**\$1.1B USD**

in ransomware payments in 2023<sup>13</sup>



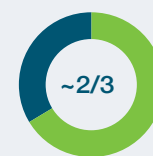
**Ransomware compromises linked to unmanaged devices**

Social engineering or error<sup>14</sup>



**Breaches involve human element**

Social engineering | error<sup>15</sup>



**Nearly 2/3 of organizations experience major security incidents that jeopardize business operations<sup>16</sup>**



**Organizations were negatively impacted by an average of 4.16 supply chain breaches in 2023<sup>17</sup>**

The threat landscape today is not made up of opportunistic actors, but of nation-state actors, criminal organizations, and hacktivists motivated by financial gain as well as a desire to disrupt and destroy. Attackers leverage sophisticated technologies, including a proliferation of low-cost toolkits that leverage machine learning and artificial intelligence.

Nation-state targeting of **critical infrastructure** has increased dramatically, representing 41% of all nation state threat notifications in 2023.<sup>18</sup> These attacks can have a debilitating impact on a nation's security, economic security, public health and/or safety.<sup>19</sup> In fact, as digital transformation exposes new risks to impacting operational technology (OT), there has been a 150% global increase in OT attacks, resulting in production outages, equipment damage and the potential for **impact to human lives**.<sup>20</sup> For example, Mitsubishi Electric announced a vulnerability that exposes its factory automation products to a risk of remote authentication bypass, if remote authentication is not replay-resistant.<sup>21</sup>

This report will examine the current global regulatory landscape for data security and privacy, the emerging focus on critical infrastructure sectors, and the regulatory shift to Zero Trust and modern strong authentication.





## Vital sectors and their impact

Although definitions of critical infrastructure vary across countries, these sectors are vital because their incapacitation or destruction would have a debilitating effect on a nation's security, economic security, public health, and/or safety which can pose a physical threat to human lives.

This includes, but is not limited to the following sectors:



## A glossary of evolving cyber attacks

Credentials are the most popular entry point for breaches,<sup>22</sup> with threat actors leveraging valid credentials to find data or compromise systems. Even in situations where cyber attacks are also multi-step, stolen credentials are generally leveraged to deploy malware or to launch a targeted phishing attack to gain additional or elevated access to systems and data. In 2023, there was a 71% increase in cyberattacks that leveraged stolen or compromised credentials.<sup>23</sup>

### Hacking



Driven by **stolen credentials**

61% of hackers are integrating AI capabilities to find more vulnerabilities<sup>24</sup>

Many threat actors leverage stolen credentials to hack target systems, primarily web applications and mail servers.

**Brute force attacks** use trial and error for common passwords (password spraying) or breached credentials (credential stuffing) to gain access to systems and networks.

**Attacker-in-the-middle** (AitM) attacks is a form of eavesdropping to spy, sabotage, or capture data—particularly credentials.

**SIM swapping** targets a weakness in traditional telephony as a form of 2FA by substituting or intercepting a call or text message to a mobile device, exploiting the ability of subscriber identity module (SIM) cards to be ported by mobile service providers from device to device bearing different telephone numbers.

### Malware



32% of breaches involved some type of extortion, including ransomware<sup>25</sup>

Software-based attack designed with malicious intent to disrupt a network or to cause damage to data and systems.

**Ransomware** attacks aim to encrypt sensitive data or systems to be held hostage. Ransomware is a growing threat, with over 57% of victims making payments to recover data or prevent its exposure.<sup>26</sup>

**Leakware** both encrypts and exfiltrates said data directly to the attacker or a nominated destination. The malicious actors then threaten to release the sensitive data to the public if the victims don't pay up before it encrypts it. The ransomware actors then threaten to release the sensitive data to the public if the victims don't pay up.

### Social Engineering



94% of organizations report being victims of phishing—91% experienced data loss and exfiltration<sup>27</sup>

Attacks that involve psychological manipulation or deception to breach traditional security measures or for targets to divulge information or take an undesirable action unwittingly.

**Phishing or spear phishing** attacks trick users into giving up sensitive information, most commonly credentials, or to install malware for staging future attacks. Modern attacks may leverage QR codes (quishing) as the lure or be aided by AI.

**OAuth phishing** tricks users to grant malicious third-party applications access to an account with valid OAuth tokens.

**MFA or push fatigue** repeatedly pushes 2FA requests to coerce users to confirm impersonator identity and grant access to accounts. Users accept out of habit, by accident, or to stop notifications.



The top 5 mobile authentication misconceptions

Get the whitepaper  
[yubi.co/mobile-auth-misconceptions-wp](https://yubi.co/mobile-auth-misconceptions-wp)

### Global standards and frameworks that support strong authentication:

NIST



fido



HITRUST



# Phishing-resistant authentication: the foundation of emerging requirements

## Key definitions, standards and frameworks

This urgent need to improve cyber defenses across all sectors is being met by global regulators. Furthermore, the evolution of modern authentication technology, in the form of the scalable FIDO2 standard and passkeys, is also having a direct impact on regulations.

Globally, regulations reflect the insufficiency of legacy forms of MFA, including requirements for strong MFA, increasingly specified as phishing-resistant MFA, and Zero Trust.

## Not all MFA is created equal

With a high rate of cyber attacks focusing on credential theft, strong MFA holds the power to drastically reduce the success of cyber attacks. MFA is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence, or factors, but not all MFA is created equal. In fact, legacy forms of MFA such as SMS, mobile authentication and one-time passcodes (OTP) experience a 10-24% attack penetration rate.<sup>28</sup>



### Something you know

Password or PIN



### Something you have

A physical device such as a phone or authenticator.



### Something you are




A fingerprint, iris or facial scan



## What are authentication assurance levels?

Standards have emerged that classify the strength of authenticators through authentication assurance levels (AALs), as defined by the National Institute for Standards and Technology (NIST),<sup>29</sup> globally recognized for promoting equitable standards. NIST standards are fundamental to US compliance, but are also directly referenced by global regulators, policy makers and industry associations or used as inspiration for similar standards, as is the case with Australia's Essential Eight Maturity Model (E8MM)<sup>30</sup> and the EU's electronic Identification, Authentication and Trust Services Regulation (eIDAS).<sup>31</sup>

The NIST guideline recognizes shifts in both risk and emerging authentication models such as phishing-resistant MFA and passkeys. While any form of MFA will provide greater security than a password (AAL1), and synced passkeys have been recognized at AAL2,<sup>32</sup> and synced passkeys have been recognized at AAL2, an authenticator at AAL3 provides very high confidence that someone logging onto your system can prove, by physical possession, who they are claiming to be, reducing the threat of compromise and attack from phishing. Relating back to AAL, only FIDO passkeys that are not synced and are properly stored in dedicated hardware have an AAL3 rating, based on a recently released NIST update to SP800-63B, providing guidance specifically on syncable authenticators. Relating back to AAL, only FIDO passkeys that are not synced and are properly stored in dedicated hardware have an AAL3 rating, based on a recently released NIST update to SP800-63B,<sup>33</sup> providing guidance specifically on syncable authenticators.

AAL1	AAL2	AAL3
<b>Single-factor authentication</b> e.g., username and password	<b>Two-step authentication</b> e.g., 2FA, synced passkeys, device-bound passkeys on general purpose devices	<b>Hardware-based multi-factor authentication</b> e.g., device-bound passkeys on hardware security keys
 <ul style="list-style-type: none"> <li>• Low security assurance</li> <li>• Highly vulnerable to phishing</li> <li>• Puts enterprises at risk</li> </ul>	 <ul style="list-style-type: none"> <li>• Phishing-resistant 2FA/MFA</li> <li>• Stronger security than a password but vulnerable to attacks</li> <li>• More enterprise-ready but leaves gaps in operational efficiency and audit/compliance requirements</li> </ul>	 <ul style="list-style-type: none"> <li>• Phishing-resistant MFA</li> <li>• Strongest security and highest assurance</li> <li>• Addresses enterprise security, operational efficiency and audit/compliance requirements</li> <li>• Supports FIDO and Smart Card/PIV</li> <li>• FIPS 140-2 validated</li> </ul>





## Cultivating phishing-resistant users

The only effective approach to remove phishing from an organization's threat landscape is to ensure that every user within the organization becomes phishing-resistant—and that resistance must move with the users no matter how they work, across devices, platforms and systems. Deploying phishing-resistant authentication across the entire user lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

## What is phishing-resistant MFA?

Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process. According to NIST Special Publication (SP) 800-63-4, currently, only two forms of authentication meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern **FIDO2/WebAuthn** authentication standard.<sup>34</sup>



## What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

- **Synced passkeys** live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.
- **Device-bound passkeys** offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

63%



of global organizations have fully or partially implemented a Zero Trust strategy<sup>35</sup>



Accelerate your Zero Trust strategy with phishing-resistant MFA

Get the whitepaper  
[yubi.co/accelerate-zero-trust-wp](https://yubi.co/accelerate-zero-trust-wp)

## Phishing-resistant MFA accelerates Zero Trust

Globally, traditional perimeter-based security models are recognized as insufficient to reduce risk or support business resiliency and continuity in modern times. Best practice security is shifting to Zero Trust, a strategy that removes ‘implicit trust’ to better protect sensitive data, systems or intellectual property. A Zero Trust strategy reduces risk by assuming all users, devices and applications are potential threats that should be verified and authenticated before access is granted.

The Zero Trust Maturity Model (ZTMM)<sup>36</sup> is a framework developed by the US Cybersecurity and Infrastructure Security Agency (CISA) that builds on NIST guidance<sup>37</sup> and recognizes that **not all forms of MFA are created equal**, requiring stronger forms of MFA be adopted for each subsequent stage, progressing toward the exclusive use of **phishing-resistant MFA**.

## The transition to ISO 27001:2022

The global ISO/IEC 27001:2022<sup>38</sup> and 27002<sup>39</sup> standards have both been revised to support the evolving risk landscape. In order to meet the October 31, 2025 deadline and ensure recertification, organizations should transition to new requirements and controls several months in advance.

The revised standards require organizations to ensure access “is controlled by [sic] secure authentication technologies and procedures to prove the identity of the user,” which is determined based on risk and must extend to third-parties, and which is supported by effective cryptographic key management. These changes allow the standard to remain in line with the latest security best practices such as Zero Trust and phishing-resistant MFA.



47.9%



of organizations believe they are succeeding at meeting compliance regulations.<sup>40</sup>

### Cyber insurance also requires MFA

Cyber insurance risk models have also been adjusted to account for increased risk levels prevalent in the current landscape, with MFA now a standard qualifier for coverage or more desirable terms or premiums.



Get the visual industry brief  
[yubi.co/cyber-insurance-vib](https://yubi.co/cyber-insurance-vib)

## The global compliance landscape

The pace of regulatory change is increasing around the globe in response to the threat landscape. Wide-sweeping directives such as the revised EU Network and Information Security (NIS) 2 Directive<sup>41</sup> will trigger a new wave of laws across the EU in 2024, with compliance requirements that begin immediately. In the US, a flurry of state privacy laws are emerging alongside new regulations, amendments and executive orders that bridge the gap federally in response to new risks to specific sectors and the supply chain.

Across the globe, the risk of impact to national security, economic stability, public health and/or safety has significantly increased the regulatory burden for the critical infrastructure and public sector organizations. Furthermore, it is increasingly common to see the private sector self-regulate with evolving governance and regulatory frameworks.

Consumer privacy concerns have also triggered a number of regulations that set minimum standards for data protection, including strong MFA, with more on the way. In the US alone, 350 consumer privacy bills were introduced across 40 US states and Puerto Rico in 2023,<sup>42</sup> with eight being enacted into law.<sup>43</sup> In 2024, five new laws will come into effect.<sup>44</sup> More broadly, the implications of GDPR can also be significant for businesses around the world; while Meta's 1.2 billion Euro GDPR fine<sup>45</sup> is the largest fine to date, this nonetheless represents only 58% of the total GDPR fines for 2023.<sup>46</sup>

The bar for strong MFA continues to get higher as threats and authentication technologies evolve. To be future-proofed against shifting compliance requirements, look to the regulations with the strongest requirements for phishing-resistant MFA, Zero Trust, and modern login flows such as passwordless.

The following sections will detail existing and emerging cybersecurity and privacy legislation or directive at the national, state or industry levels (some of which have global implications) that specifically call out a requirement for authentication, access controls, or Zero Trust. Information in the following sections will be

#### Global

Broader scope

#### North America

United States,  
Canada

#### Europe & the UK

EU countries, United  
Kingdom, Switzerland

#### Asia Pacific

Japan, Singapore,  
India, Australia,  
New Zealand



## National and state regulations

These regulations are designed to govern the storage and use of personally identifiable data, within the context of an individual's privacy rights. They apply to qualifying organizations across an entire country or to a state within a country.

Where requirements state “appropriate” or “reasonable” safeguards be implemented, enforcement actions are often a better barometer for specific requirements. Best practice suggests adopting the highest possible standard to avoid potential non-compliance fines.

### Consumer data privacy legislation

	Country	Regulation	Applies to	Requirements
North America	United States	<b>State laws:</b> California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia. <sup>47</sup>	Residents of each state	The majority specify the need for “reasonable administrative, technical, and physical data security practices.” <sup>48</sup>
	United States	<b>FTC Act</b> Federal Trade Commission Act <sup>49</sup>	All U.S. residents	Broad empowerment to enforce privacy. Recent orders include provisions for phishing-resistant MFA or passkeys for all employees, contractors and affiliates and the requirement to enable MFA for consumers. <sup>50</sup>
	Canada	<b>PIPEDA</b> The Personal Information Protection and Electronic Documents Act <i>Supplemented by provincial privacy acts.</i>	All private sector organizations	Requires “appropriate identification and authentication processes,” with enforcement leaning to “authenticators should not be easily replicated or spoofed.” <sup>51</sup>
Europe & the UK	All EU countries	<b>GDPR</b> General Data Protection Regulation <i>National laws within the EU often incorporate GDPR elements, e.g. the BDSG-new Federal Data Protection Act (Bundesdatenschutzgesetz) in Germany<sup>52</sup> and the FDPA French Data Protection Act in France.<sup>53</sup></i>	All EU and European Economic Area (EEA) data subjects, regardless if they are in the EU or EEA	Data protection by design and default. “Appropriate technical and organizational measures” to protect and secure data. <sup>54</sup> ENISA guidelines suggest two-factor authentication. <sup>55</sup> Enforcement actions have indicated a requirement for MFA. <sup>56</sup>
	United Kingdom	<b>UK GDPR</b> Data Protection Act 2018	UK data subjects	Requires “appropriate security of the personal data,” requiring periodic review, <sup>57</sup> recommended to be MFA. <sup>58</sup>
	Switzerland	<b>nFADP</b> New Federal Act on Data Protection (2023)	Swiss natural persons	Requires appropriate organizational measures, including authentication. <sup>59</sup>



## Consumer data privacy legislation

	Country	Regulation	Applies to	Requirements
Asia Pacific	India	<b>DPDP or DPDPA</b> Digital Personal Data Protection Act (2023)	All India data subjects, regardless if they are in India	Implement “security safeguards.” <sup>60</sup>
	Japan	<b>APPI</b> The Act on the Protection of Personal Information	All Japanese data subjects, regardless if they are in Japan	Use “necessary and appropriate measures” to prevent data leakage, loss or damage. <sup>61</sup>
	Singapore	<b>PDPA</b> Personal Data Protection Act	All private sector organizations in Singapore	Suggest MFA for admin access, <sup>62</sup> with enforcement requiring MFA for admin and remote access. <sup>63</sup>
	New Zealand	<b>Privacy Act 2020</b>	New Zealand data subjects	Reasonable security safeguards, <sup>64</sup> encourages two-factor authentication for all agencies. <sup>65</sup>







## Cybersecurity legislation

These cybersecurity regulations have implications for organizations across sectors, encompassing all publicly traded companies or all critical infrastructure organizations.

In addition to regulatory requirements, most critical infrastructure providers adhere to the best practices of advisory groups such as the global *Identifying and Mitigating Living Off the Land Techniques*<sup>66</sup> co-created between agencies in the US, Australia, Canada, the UK and New Zealand, in addition to the Ensuring Security Framework (ESF)<sup>67</sup> created in the US, both of which advocate for phishing-resistant MFA to protect critical infrastructure.

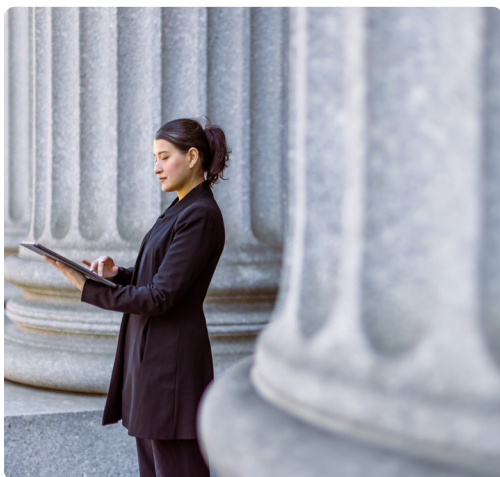
	Country	Regulation	Applies to	Requirements
Global	All NATO nations	<b>NATO Directive on Classified Project and Industrial Security</b> North Atlantic Council	NATO Industry contractors	Two-factor authentication required when physical security measures are not present. <sup>68</sup>
	United States	<b>SOX</b> Sarbanes-Oxley Act	All publicly traded companies, some private companies	General advice to keep data “secure” and enforce access controls. <sup>69</sup> However, SOX is based on SOC 2 (Service Organization Control), which favors multi-factor authentication (MFA). <sup>70</sup>  Potential for shifts in audit themes to reflect new needs (remote work).
North America	United States	<b>NSM-22</b> Critical Infrastructure Security and Resilience Replaces PPD-21	16 critical infrastructure sectors	Directs the establishment of sector-specific and cross-sector security requirements consistent with the National Cybersecurity Strategy <sup>71</sup> by March 13, 2025, <sup>72</sup> including Zero Trust and MFA.
	Canada	<b>CCSPA</b> Critical Cyber Systems Protection Act (bill pending)	Vital services <i>Telecommunications, energy, transportation, financial</i>	Establish a Cyber Security Program and mitigate supply chain risks.  Requirements not yet detailed. <sup>73</sup>

## Cybersecurity legislation

Country	Regulation	Applies to	Requirements
Europe & the UK	All EU countries	<b>EU Cybersecurity Act</b> <sup>74</sup>	All information and communications technology (ICT) products, services and processes
	All EU countries	<b>eIDAS 2.0</b> Electronic IDentification, Authentication, and Trust Services (2024) Framework for <b>European digital identity (eID)</b> <sup>76</sup>	<p>Defines Levels of Assurance (LoA) for digital identity verification:</p> <p>Level “substantial” requires two-factor authentication and dynamic authentication.</p> <p>Level “high” requires protections against duplication, tampering and attacks and an authentication mechanism that is resistant to attack, e.g. smart cards or hardware tokens such as a FIDO security key.<sup>77</sup></p>
	All EU Countries, Norway, Iceland and Ukraine	<b>NIS / NIS2</b> Network and Information Security Directive <sup>78</sup>	<p>Operators of essential services, relevant digital services providers carried out in the EU, regardless of where the organization is based</p> <p>Requirements include the adoption of “cyber hygiene practices, such as zero-trust principles” and risk-management measures that must include MFA.<sup>79</sup></p> <p>Requires member states to transpose requirements into national law by October 2024.</p>
	All EU Countries	<b>CER</b> Critical Entities Resilience (CER) Directive	<p>Critical infrastructure</p> <p>Ensure adequate access controls for direct and remote access.<sup>80</sup></p> <p>All member states to publish measures by October 17, 2024.</p>
	Germany	<b>BSI-KritisV</b> BSI Ordinance Determining Critical Infrastructure	<p>Critical infrastructure</p> <p>Requires “state of the art” protection measures.<sup>81</sup></p>

## Cybersecurity legislation

	Country	Regulation	Applies to	Requirements
Europe & the UK	Germany	<b>IT Security Act 2.0</b> May 2023 <i>Amends the Federal Security Act (Bundessicherheitsgesetz "BSIG")</i>	Government and critical infrastructure	Will require information security above and beyond ISO 27001. <sup>82</sup> *NIS2 requirements will likely trigger the IT Security Act 3.0
	Switzerland	<b>ISG</b> Information Security Act (Informationssicherheitsgesetz) 2024	Federal government, critical infrastructure	Restrict access to authorized persons, only when needed, with protections from misuse, commensurate to risk. <sup>83</sup>
Asia Pacific	Australia	<b>SOCI Act</b> Security of Critical Infrastructure Act	Critical infrastructure	Minimize or eliminate cyber risks to digital systems, computers, datasets or networks, including improper access. <sup>84</sup> <b>Essential Eight Maturity Model (E8MM)</b> <sup>85</sup> Level 2+ requires phishing-resistant MFA
	Japan	<b>NISC Guidance</b> National Center of Incident Readiness and Strategy for Cybersecurity	Critical infrastructure	Move toward the use of stronger authentication, specifically mentioning FIDO2/WebAuthn, and emphasizes the risks with weaker forms of MFA, such as AiTM attacks, MFA fatigue, and SIM swapping. <sup>86</sup>
	Singapore	<b>Cybersecurity Act 2018</b>	Critical information infrastructure	Requires Zero Trust and MFA for privileged accounts and remote access <sup>87</sup>



## Public Sector

While the public sector is narrowly defined in the US, the global scope for the public sector includes many additional sectors under federal jurisdiction including, but not limited to, healthcare, education, telecommunications and transportation.

The public sector in the United States is bound by a complex series of regulations, executive orders, and detailed NIST standards and publications, arguably setting a new global bar for protecting the public sector with Zero Trust and phishing-resistant MFA.

Although only the US public sector is bound to these evolving NIST standards, the standards outlined below are referenced globally, particularly within critical infrastructure sectors such as manufacturing, financial services and healthcare. In fact, the Cyber Safety Review Board (CSRB), recommends all private and public “organizations urgently implement improved access controls and authentication methods and transition away from voice and SMS-based MFA; those methods are particularly vulnerable. Instead, organizations should adopt easy-to-use, secure-by-default, passwordless solutions such as Fast Identity Online (FIDO)2-compliant, phishing-resistant MFA methods.”<sup>88</sup>

Country	Regulation	Applies to	Requirements
North America	United States  <b>Computer Security Act</b> <b>Clinger-Cohen Act</b> <b>HSPD-12</b> Homeland Security Presidential Directive 12	Federal agencies	Adhere to the following Federal Information Processing Standards (FIPS):  <b>FIPS 201-3 PIV Personal Identity Verification of Federal Employees and Contractors<sup>89</sup></b> MFA required to authenticate user; options for strong alternatives to the PIV and CAC overseen by <b>OMB M-19-17<sup>90</sup></b> and <b>M-20-19<sup>91</sup></b>  <b>FIPS 140-2 (to 2026), 140-3<sup>92</sup> Security Requirements for Cryptographic Modules</b> Certifiable security levels for third-party software or services, Level 4 being most secure.
	United States  <b>EO 14028</b> Executive Order on “Improving the Nation’s Cybersecurity” <sup>93</sup>	Federal agencies and their supply chain partners	<b>OMB M-22-09<sup>94</sup> &amp; NSM-8<sup>95</sup></b> Requires a phishing-resistant authenticator that meets AAL2 standards at minimum by end of FY2024 as part of deploying Zero Trust.  <b>SP 800-207 Zero Trust Architecture<sup>96</sup></b> Assumes no implicit trust, requires phishing-resistant MFA.  <b>OMB M 21-30<sup>97</sup> &amp; NIST Security Measures for “EO-Critical Software”<sup>98</sup></b> Use MFA that is impersonation resistant for all users and administrators of EO-critical software.

## Public Sector

Country	Regulation	Applies to	Requirements
North America	United States	FISMA Federal Information Security Modernization Act	Federal agencies
			<p><b>Draft SP 800-63-4 Digital Identity Guidelines</b><sup>99</sup> Redefines AALs, recognizes two forms of phishing-resistant MFA: channel binding (used by Smart Cards) and verifier name binding (used by FIDO2)</p> <p><b>SP 800-157r1 Guidelines for Derived PIV Credentials &amp; SP 800-217 Guidelines for PIV Federation</b><sup>100</sup> Guidelines for PKI credentials for PIV and new methods on how to implement FIDO2 and federation.</p> <p><b>SP 800-171r2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations</b><sup>101</sup> MFA required for all authorized users who access controlled unclassified information (CUI)</p>
	United States	FedRAMP program The Federal Risk and Authorization Management Program FedRAMP Authorization Act & FISMA	Federal agencies and cloud service providers
	United States	DFARS Defense Federal Acquisition Regulation Supplement to the Federal Acquisition Regulation (FAR) <b>CMMC 2.0</b> Cybersecurity Maturity Model Certification per DFARS	Contractors in the Defense Industrial Base
	Canada	Directive on Service and Digital	Government organizations

### Draft SP 800-63-4 Digital Identity Guidelines<sup>99</sup>

Redefines AALs, recognizes two forms of phishing-resistant MFA: channel binding (used by Smart Cards) and verifier name binding (used by FIDO2)

### SP 800-157r1 Guidelines for Derived PIV Credentials & SP 800-217 Guidelines for PIV Federation<sup>100</sup>

Guidelines for PKI credentials for PIV and new methods on how to implement FIDO2 and federation.

### SP 800-171r2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations<sup>101</sup>

MFA required for all authorized users who access controlled unclassified information (CUI)

### SP 800-53r5<sup>102</sup>

Implement MFA to standards in 800-63-4

### DFARS 204.7302<sup>103</sup>

Contractors required to implement NIST SP 800-171, MFA required

### CMMC FAR 52.204-21<sup>104</sup>

Level 2 requires practices aligned to NIST 800-171, MFA required

Level 3 requires practices aligned to NIST SP 800-171 and supplemental 800-172,<sup>105</sup> requiring authentication that is cryptographically based and replay (phishing) resistant

“Protecting information and data by documenting and mitigating risks.”<sup>106</sup>



## Public Sector

	Country	Regulation	Applies to	Requirements
Europe & the UK	UK	<b>GovS 007: Security</b> Government Functional Standard	Government agencies and critical infrastructure	Access to classified, sensitive or critical information and key operational services should be limited to “authenticated and authorized users” with “proportionate risk mitigation controls.”  <b>Cyber Assessment Framework</b> Identity and access controls progress toward MFA for privileged and remote access <sup>107</sup>
	UK	<b>PPN</b> Procurement Policy Note	Supply chain partners	<b>Cyber Essentials certification (2023)</b> MFA required for admin accounts and all access cloud services <sup>108</sup>
Asia Pacific	Japan	<b>Common Standards for Cybersecurity Measures for Government Agencies</b>	Government Agencies	Choose authentication based upon risk, <sup>109</sup> MFA suggested. <sup>110</sup>
	Australia	<b>The Privacy Act 1988</b> 2022 Amendment	Australian agencies and their partners, health services, large private organizations	Implement “security safeguards as it is reasonable in the circumstances to take.” <sup>111</sup>





## Finance

The Finance industry has globally set the bar for strong authentication, in part due to the global PCI-DSS standard, which includes new requirements for phishing-resistant MFA for all access to the cardholder data environment.<sup>112</sup>

The financial sector is also stepping up consumer protections with the introduction of phishing-resistant MFA and passkeys. In October 2023, The Monetary Authority of Singapore's (MAS) Cyber Security Advisory Panel (CSAP) issued support for consumer use of MFA and passwordless authentication.<sup>113</sup> In 2022, a Consumer Financial Protection Bureau circular suggested that MFA solutions that protect against credential phishing are “especially important” and should be considered for consumer account protection.<sup>114</sup>

“MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee's smart phone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA.”

**New York Department of Financial Services | Twitter Investigation Report | October 2020**

	Country	Regulation	Applies to	Requirements
Global	Global	<b>PCI DSS 4.0.1</b> The Payment Card Industry Data Security Standard	Any global business that accepts, handles, stores or transmits cardholder data	Phishing-resistant MFA for access to the cardholder data environment. <sup>115</sup>  New requirements effective March 31, 2025.

## Finance

	Country	Regulation	Applies to	Requirements
North America	United States	<b>GLB Act / GLBA</b> Gramm-Leach-Bliley Act Safeguards Rule (16 CFR 314) <sup>116</sup>	Financial institutions	Requires MFA for employee and customer access to systems. <sup>117</sup>
	United States	<b>FFIEC</b> Federal Financial Institutions Examination Council	Consumers of financial products	Guidance that single-factor authentication is inadequate and that MFA be considered. <sup>118</sup> Suggests MFA be prioritized for digital banking consumers engaging in high-risk transactions and that hardware-based MFA be prioritized for high-risk users. <sup>119</sup>
	United States	<b>Dodd-Frank Act</b>	Financial services industry	A Consumer Financial Protection Bureau (CFPB) circular urges transition to MFA for employees and as an option consumer accounts, stating that the lack of MFA could trigger liability under CFPB regulations or even the Dodd-Frank Act, even in the absence of a data breach. <sup>120</sup>
	United States	<b>SEC Final Rule</b> Securities Exchange Commission 17 CFR Parts 229, 232, 239, 240 and 249	Advisors and funds	Include cybersecurity processes for managing risk. <sup>121</sup>
Europe & the UK	All EU Countries	<b>PSD2</b> EU Payment Services Directive 2	Card issuers and banks within the EU and EEA	Requires “dynamic linking” that links the payee to the user through strong authentication. <sup>122</sup>
	All EU Countries	<b>DORA</b> Digital Operational Resilience Act	Financial entities, impact on technology and telecommunications	ICT risk management and governance, to ensure systems and data are “adequately protected from risks including damage and unauthorized access or usage”. Third-party risk management. <sup>123</sup> Requirements apply January 17, 2025 <sup>124</sup>



## Health & pharmaceuticals

The health sector is subject to a growing number of regulations targeting healthcare delivery organizations, pharmaceuticals and health technology (e.g. ISO standards, EU and UK Medical Device Regulations, and the Medical Device Single Audit Program). In the US, the White House is currently working with the Department of Health and Human Services to create new minimum cyber standards for healthcare.<sup>125</sup>

Here are some of the regulations specifically related to health delivery and pharmaceuticals:

Country	Regulation	Applies to	Requirements
North America	<b>United States</b>  <b>HIPAA Security Rule</b> The Health Insurance Portability and Accountability Act  <b>The HIPAA Safe Harbor Bill (HR 7898)</b> <i>Amends the HITECH Act</i>	Healthcare organizations	“Reasonable” physical, technical, and administrative safeguards for data security and authentication. <sup>126</sup>  Safe Harbor requires “recognized security practices,” defined by NIST, and asks regulators to consider these standards when looking at audits and fines. <sup>127</sup>  <b>NIST SP 800-66r2 Implementing HIPAA (2024)</b> Consider MFA & ensure authentication mechanisms are protected from inappropriate manipulation. <sup>128</sup>
	<b>United States</b>  <b>FDA CFR 21 Part 11</b> Code of Federal Regulations Title 21 — Food and Drugs		Requires certification that e-signatures in their systems are legally binding.  A 2020 revision requires certification to use 2FA or MFA in compliance with FIPS 140-2. <sup>129</sup>
	<b>United States</b>  <b>Support Act / EPCS</b> Electronic Prescription for Controlled Substances <i>Regulated by the Drug Enforcement Administration (DEA)</i>		The use of mobile devices requires two-factor authentication (hard token preferred), and a device compliant with FIPS 140-2. <sup>130</sup>
	<b>United States</b>  <b>CURES Act Final Rule</b>	Healthcare industry	To support the secure access and exchange of electronic health information, with certification of health IT related to encrypting authentication credentials or MFA. <sup>131</sup>



## Critical infrastructure sectors

Energy and natural resources, transportation, telecommunications, water supply, manufacturing

Following high-profile attacks, a number of critical infrastructure sectors in the US received security directives; over time, these are likely to be replaced by a more comprehensive National Cybersecurity Strategy.<sup>132</sup> In the interim, sectors are conforming to new baselines that include phishing-resistant MFA such as those from the National Association of Regulatory Utility Commissioners and the US Department of Energy.<sup>133</sup> The UK National Cyber Strategy also recognizes gaps in legislation related to critical infrastructure that will likely be amended.<sup>134</sup>

Critical infrastructure organizations around the world look to ISO standards for critical infrastructure protection, including 62443, 22301, 27035, 27005, 15408 and 27001 as well as FIPS 140-1 and 186-3.<sup>135</sup> As digital transformation has eroded the traditional network protections for OT-dependent organizations, new requirements are supporting the shift to Zero Trust.

	Country	Regulation	Applies to	Requirements
North America	United States	<b>Federal Power Act</b> 18 CFR 39.7	Energy sector	<b>NERC CIP</b>  Critical Infrastructure Protection Standards 007-6, 005-6 Enforce authentication for access controls. Require MFA for all remote access sessions. <sup>136</sup>
	United States	<b>TSA Security Directive Pipeline 2021-01 series</b> Transportation Security Administration First Directive	Pipeline sector	Identify and report on cybersecurity gaps, <sup>137</sup> implement access controls for IT and OT, <sup>138</sup> refer to CISA's guidance to adopt MFA. <sup>139</sup>
	United States	<b>TSA Security Directive Pipeline 2021-02 series</b> Second Directive (revised 2023)	Pipeline sector	Implement immediate mitigation measures against cyberattacks consistent with NIST SP 800-82 and Zero Trust. <sup>140</sup>



Critical infrastructure sectors

	Country	Regulation	Applies to	Requirements
North America	United States	<b>TSA Security Directive 2022-01</b>	Rail operations	Eliminates domain trust between IT and OT systems. Requires the use of MFA. <sup>141</sup>
	United States	<b>TSA Security Directive 2023-03</b>	Airport and aircraft operators	Implement access controls consistent with the National Cybersecurity Strategy. <sup>142</sup>
	United States	<b>EPA M-2023-11*</b> Environmental Protection Agency	Water Systems	Ensure the adequacy of cybersecurity for OT systems, specifically closing gaps on stolen credentials, insecure remote access, and third-party vulnerabilities. <sup>143</sup> <i>Memo was rescinded, now stands as best practice.</i>
Europe & the UK	UK	<b>Telecommunications (Security) Act 2021</b>	Telecommunications sector	Take security measures to avoid unauthorized access. <sup>144</sup>
	All digital products sold in the EU	<b>Cyber Resilience Act (CRA)</b> (pending)	Manufacturing sector (digital products)	Products with digital elements must ensure protection from unauthorised access, including authentication. <sup>145</sup> Manufacturers will have 36 months to comply.
Asia-Pacific	Australia	<b>AESCSF</b> Australian Energy Sector Cyber Security Framework <sup>146</sup>	Energy sector	Leverages the US Department of Energy’s Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the NIST Cybersecurity Framework (NIST CSF); speaks to the importance of Zero Trust. <sup>147</sup>
	Malaysia	<b>Cyber Security Act</b>	Critical infrastructure	National Cybersecurity Agency (NACSA) is encouraging FIDO security keys for companies and agencies associated with critical infrastructure. <sup>148</sup>

## The total economic impact of YubiKeys:



### Strongest Security

Reduce risk by

**99.9%**



### High Return

Experience ROI of

**203%**



### More Value

Reduce support tickets by

**75%**



### Faster

Decrease time to authenticate by

**>4x**



### Durable

IP68 rated, crush resistant, no battery required, no moving parts

# YubiKey offers high-assurance, phishing-resistant MFA helping enterprises cultivate phishing-resistant users

MFA investments must provide organizations with protection that evolves alongside risk and compliance requirements. Yubico offers the YubiKey, a hardware security key that affords highest-assurance, phishing-resistant MFA supporting both FIDO2/WebAuthn and Smart Card/PIV authentication to ensure the highest protection against phishing and other credential-based attacks to help future-proof your MFA investment. The YubiKey enables you to cultivate phishing-resistant users, providing authentication that moves effortlessly with users no matter how they work.

By safeguarding registration, authentication, and recovery across all devices, platforms, and processes with YubiKeys enterprises build the highest-assurance foundation to combat evolving threats. The YubiKey is designed to meet you where you are on your authentication journey, offering multi-protocol support that also extends to FIDO U2F, HOTP/TOTP and OpenPGP. For the most regulated industries, we offer the YubiKey FIPS Series offering certified and validated protection enabling government agencies and regulated industries to meet the highest authenticator assurance level 3 (AAL3) requirements from the new NIST SP800-63B guidance.



### The YubiKey FIPS Series

140-2 validated, DOD-approved<sup>149</sup> and meets the highest AAL3 level.

Hardware security keys such as the YubiKey are an ideal option for IT, OT and ICS access because they don't require additional hardware, software, external power, batteries, or even a network connection—a single key secures thousands of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.

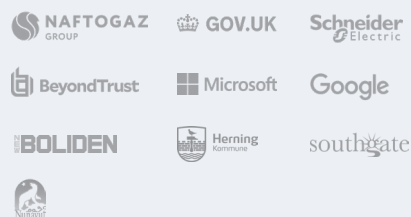
As a portable hardware root of trust, the YubiKey is proven to **reduce risk against phishing attacks and account takeovers by 99.9%**<sup>150</sup> and serves as a user-friendly, cost-effective enabler of a Zero Trust security architecture. When you're ready, the YubiKey can also help bridge to modern login flows such as passwordless.

## Takeaway

While it is true that regulations are putting pressure on organizations around the world to adopt strong MFA and even Zero Trust, these mandates are both necessary and timely to address growing cyber threats and the usability challenges associated with passwords and legacy MFA. Around the world, 66% of enterprises either have, are piloting or are planning to deploy **passwordless authentication** within the next year.<sup>151</sup>

Passwordless authentication is any form of authentication that doesn't require the user to provide a password at login. Going passwordless is a journey for most organizations, not necessarily an overnight change—first moving away from passwords and legacy forms of MFA, which are all highly vulnerable to phishing, and then moving to a modern MFA approach which offers strong phishing-defense. Once there, an organization is well poised to transition completely to passwordless.

**The YubiKey is a bridge solution that can help support today's password problem and build toward the secure, phishing-resistant and passwordless future.**



Learn more customer stories  
[yubi.co/customers](https://yubi.co/customers)



Learn more about  
how to deploy  
phishing-resistant  
MFA with  
the YubiKey



Get the best practice guide  
[yubi.co/bpgg-mfa](https://yubi.co/bpgg-mfa)



# A Best Practice Checklist for Security and Compliance



## Embrace zero trust

Treat each access request as a potential attack and authenticate the user before providing access to the network or any sensitive resource



## Know your data

Manage your data retention policy and keep only what you need for long-term compliance mandates



## Secure user access

Use MFA to access all IT systems and implement phishing-resistant authentication for all privileged users



## Design security with UX in mind

Deploy solutions that are user friendly and are accessible across devices, anywhere, anytime



## Educate, educate, educate

Combine technology with employee education to spot and stop phishing and spear phishing attacks



## Stay updated

Apply software patches for all high-risk vulnerabilities within 30 days, and use only supported software versions



## Put privacy first

Most regulations are moving toward consumer rights, so be prepared to meet them



## Think long term

Deploy solutions that work across legacy and modern infrastructures; they shouldn't become obsolete if existing regulations are updated, or new regulations are released

## Sources

- <sup>1</sup> PCI, PCI DSS v4.0.1, (2024), [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\\_0.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf)
- <sup>2</sup> CPO Magazine, Top Privacy and Cybersecurity Issues to Track in 2024, (Accessed April 10, 2024), <https://www.cpomagazine.com/data-privacy/top-privacy-and-cybersecurity-issues-to-track-in-2024/>
- <sup>3</sup> Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
- <sup>4</sup> White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 2022), <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/?mod=djemCIO>
- <sup>5</sup> NIST, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, (February 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf>
- <sup>6</sup> European Parliament, The NIS2 Directive, (February 2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- <sup>7</sup> European Commission, Digital Operational Resilience Act (Accessed April 10, 2024), [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)
- <sup>8</sup> Council of the EU, European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans, (March 26, 2024), <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>
- <sup>9</sup> Ministry of Law and Justice, DPDPA-2023, (August 11, 2023), <https://egazette.gov.in/WriteReadData/2023/248045.pdf>
- <sup>10</sup> Australian Signals Directorate, Essential Eight Maturity Model, (November 2023) <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>
- <sup>11</sup> NISC, The Guidance on Operations of Cybersecurity Measures of Government Agencies and Related Agencies, 2023 (Japanese), <https://www.nisc.go.jp/pdf/policy/general/guider6.pdf>
- <sup>12</sup> IBM, 2024 Cost of Data Breach Report, (August 26, 2024), <https://www.ibm.com/reports/data-breach>
- <sup>13</sup> Chainalysis, Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline, (February 7, 2024), <https://www.chainalysis.com/blog/ransomware-2024/>
- <sup>14</sup> Microsoft, Microsoft Digital Defense Report 2023, (November 8, 2023), <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023?rtc=1>
- <sup>15</sup> Verizon, 2024 Data Breach Investigations Report, (May 1, 2024), <https://www.verizon.com/business/resources/reports/dbir/>
- <sup>16</sup> Cisco, Security Outcomes Report Volume 3, (March 20, 2023), <https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html>
- <sup>17</sup> BlueVoyant, The State of Supply Chain Defense Annual Global Insights Report 2023, (December 11, 2023), <https://www2.bluevoyant.com/TheStateofSupplyChainDefense2023Report>
- <sup>18</sup> Microsoft, Microsoft Digital Defense Report 2023, (November 8, 2023), <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023?rtc=1>
- <sup>19</sup> CISA, Critical Infrastructure Sectors, (Accessed October 24, 2023), <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
- <sup>20</sup> Waterfall, 2023 Threat report - OT Cyberattacks with Physical Consequences, (May 4, 2023), <https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2023-threat-report-ot-cyberattacks-with-physical-consequences/>
- <sup>21</sup> Eduard Kovacs, Mitsubishi Electric Factor Automation Flaws Expose Engineering Workstations, (February 5, 2024), <https://www.securityweek.com/mitsubishi-electric-factory-automation-flaws-expose-engineering-workstations/>
- <sup>22</sup> Verizon, 2024 Data Breach Investigations Report, (May 1, 2024), <https://www.verizon.com/business/resources/reports/dbir/>
- <sup>23</sup> IBM, IBM X-Force Threat Intelligence Index 2024, (February 21, 2024), <https://www.ibm.com/reports/threat-intelligence>
- <sup>24</sup> Hackerone, 7th Annual Hacker-Powered Security Report, (October 15, 2023) <https://www.hackerone.com/reports/7th-annual-hacker-powered-security-report>
- <sup>25</sup> Verizon, 2024 Data Breach Investigations Report, (May 1, 2024), <https://www.verizon.com/business/resources/reports/dbir/>
- <sup>26</sup> Cyberedge Group, Cyberthreat Defense Report, (Accessed May 18, 2021), <https://cyber-edge.com/cdr/>
- <sup>27</sup> Egress, Email Security Risk Report 2024, (March 2024), [https://www.egress.com/media/o1sbpq5t/egress\\_email\\_security\\_risk\\_report\\_2024.pdf](https://www.egress.com/media/o1sbpq5t/egress_email_security_risk_report_2024.pdf)
- <sup>28</sup> Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>
- <sup>29</sup> NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf>
- <sup>30</sup> Australian Signals Directorate, Essential Eight Maturity Model, (November 23, 2023) <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>
- <sup>31</sup> European Commission, eIDAS Levels of Assurance (LoA), (2014), <https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance>
- <sup>32</sup> NIST, NIST SP 800-63Bsup1, (April 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63Bsup1.pdf>
- <sup>33</sup> NIST, Giving NIST Digital Identity Guidelines a Boost: Supplement for Incorporating Syncable Authenticators, (April 2024), <https://www.nist.gov/blogs/cybersecurity-insights/giving-nist-digital-identity-guidelines-boost-supplement-incorporating>
- <sup>34</sup> NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf>
- <sup>35</sup> Gartner, Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy, (April 22, 2024), <https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy>
- <sup>36</sup> CISA, Zero Trust Maturity Model v 2.0, (April 2023), [https://www.cisa.gov/sites/default/files/2023-04/zero\\_trust\\_maturity\\_model\\_v2\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)
- <sup>37</sup> NIST, SP 800-207 Zero Trust Architecture, (August 2020), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- <sup>38</sup> ISO, ISO/IEC 27001:2022, (October 2022), <https://www.iso.org/standard/27001>



## Sources

- <sup>39</sup> ISO, ISO/IEC 27002:2022, (February 2022), <https://www.iso.org/standard/75652.html>
- <sup>40</sup> Cisco, The 2021 Security Outcomes Study, (Accessed May 14, 2021), [https://www.cisco.com/c/m/en\\_us/products/security/cybersecurity-reports/security-outcomes-executive-summary.html](https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/security-outcomes-executive-summary.html)
- <sup>41</sup> European Parliament, The NIS2 Directive, (February 2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- <sup>42</sup> National Conference of State Legislatures, 2023 Consumer Data Privacy Legislation, (September 28, 2023), <https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation>
- <sup>43</sup> CPO Magazine, Top Privacy and Cybersecurity Issues to Track in 2024, (Accessed April 10, 2024), <https://www.cpomagazine.com/data-privacy/top-privacy-and-cybersecurity-issues-to-track-in-2024/>
- <sup>44</sup> National Conference of State Legislatures, 2023 Consumer Data Privacy Legislation, (September 28, 2023), <https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation>
- <sup>45</sup> EDPB, 1.2 billion euro fine for Facebook as a result of EDPB binding decision, (May 22, 2023), [https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision\\_en](https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en)
- <sup>46</sup> Enforcement Tracker, Fines imposed over time, (April 2024), <https://www.enforcementtracker.com/?insights>
- <sup>47</sup> National Conference of State Legislatures, 2023 Consumer Data Privacy Legislation, (September 28, 2023), <https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation>
- <sup>48</sup> Delaware, House Bill No. 154, (September 11, 2023), <https://www.whitecase.com/insight-alert/delaware-comprehensive-data-privacy-law>
- <sup>49</sup> FTC, Federal Trade Commission Act, (Accessed April 15, 2024), <https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-ac>
- <sup>50</sup> FTC, Security Principles: Addressing underlying causes of risk in complex systems, (February 1, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>
- <sup>51</sup> Office of the Privacy Commissioner of Canada, Guidelines for identification and authentication, (June 2016), [https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth\\_061013/](https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth_061013/)
- <sup>52</sup> Federal Law Gazette, Federal Data Protection Act, (BDSG), (June 23, 2021), [https://www.gesetze-im-internet.de/englisch\\_bdsge/englisch\\_bdsge.html](https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.html)
- <sup>53</sup> Olivier Proust, French legislator amends French Data Protection Act, (November 1, 2019), <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/french-legislator-amends-french-data-protection-act>
- <sup>54</sup> Intersoft Consulting, General Data Protection Regulation, (Accessed May 19, 2021), <https://gdpr-info.eu/art-32-gdpr/>
- <sup>55</sup> ENISA, Guidelines for SMEs on the security of personal data processing, (January 27, 2017), <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>
- <sup>56</sup> GDPR Enforcement Tracker, Transavia ETid 902, (November 12, 2021), <https://www.enforcementtracker.com/ETid-902>
- <sup>57</sup> Legislation.gov.uk, Data Protection Act 2018, (April 15, 2024), <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- <sup>58</sup> Legal Aid Agency, Data Security Guidance, (September 2023), [https://assets.publishing.service.gov.uk/media/65001bf757278000d251950/Provider\\_Data\\_Security\\_Guidance\\_September\\_2023.pdf](https://assets.publishing.service.gov.uk/media/65001bf757278000d251950/Provider_Data_Security_Guidance_September_2023.pdf)
- <sup>59</sup> FDPIC, nFADP main provisions, (January 12, 2024), <https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/ndsg.html>
- <sup>60</sup> Ministry of Law and Justice, DPDP-2023, (August 11, 2023), <https://egazette.gov.in/WriteReadData/2023/248045.pdf>
- <sup>61</sup> Japanese Law, Act on the Protection of Personal Information, (May 30, 2003), <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en>
- <sup>62</sup> PDPC, Guide to Data Protection Practices for ICT Systems, (Accessed April 16, 2024), <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/guide-to-data-protection-practices-for-ict-systems.pdf>
- <sup>63</sup> PDPC, Undertaking by Nippon Express Group, (July 14, 2022), <https://www.pdpc.gov.sg/undertakings/undertaking-by-nippon-express-group>
- <sup>64</sup> Privacy Commissioner, Principle 5 - storage and security of information, (Accessed April 16, 2024), <https://www.privacy.org.nz/privacy-act-2020/privacy-principles/5/>
- <sup>65</sup> Privacy Commissioner, Office of the Privacy Commissioner encourages two-factor authentications in war on cybercrime, (June 7, 2023), <https://www.privacy.org.nz/publications/statements-media-releases/office-of-the-privacy-commissioner-encourages-two-factor-authentication-in-war-on-cybercrime/>
- <sup>66</sup> CISA, Identifying and Mitigating Living Off the Land Techniques, (February 2024), <https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques>
- <sup>67</sup> CISA and the NSA, Enduring Security Framework (Accessed October 23, 2023), <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Enduring-Security-Framework/>
- <sup>68</sup> NATO, Directive on Classified Project and Industrial Security, (May 13, 2015), [https://www.nbu.cz/download/pravni-predpisy---nato/AC\\_35-D\\_2003-REV5.pdf](https://www.nbu.cz/download/pravni-predpisy---nato/AC_35-D_2003-REV5.pdf)
- <sup>69</sup> US Public Law, Public Law 107-204, (July 2002), <https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>
- <sup>70</sup> Imperva, SOC 2 Compliance, (Accessed 2024), <https://www.imperva.com/learn/data-security/soc-2-compliance/>
- <sup>71</sup> The White House, National Cybersecurity Strategy, (March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- <sup>72</sup> The White House, NSM-8, (April 30, 2024), <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>
- <sup>73</sup> House of Commons Canada, Bill C-26, (June 14, 2022), <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading>
- <sup>74</sup> The EU Cybersecurity Act (18 April 2023), <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- <sup>75</sup> ENISA, Authentication Methods, (Accessed May 20, 2021), <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods>
- <sup>76</sup> Council of the EU, European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans, (March 26, 2024), <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>

## Sources

- <sup>77</sup> Office of the European Union, Commission Implementing Regulation (EU) 2015/1502, (September 2015), <https://op.europa.eu/en/publication-detail/-/publication/1f850e61-1dd0-11ed-8fa0-01aa75ed71a1>
- <sup>78</sup> European Parliament, The NIS2 Directive, (February 2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- <sup>79</sup> European Parliament, Directive (EU) 2022/2555 of the European Parliament and of the Council, (December 14, 2022), <https://eur-lex.europa.eu/eli/dir/2022/2555>
- <sup>80</sup> Official Journal of the European Union, Directive 2022/2557, (December 14, 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/>
- <sup>81</sup> Enisa, IT Security Act (Germany) and EU General Data Protection Regulation: Guideline “State of the art”, (2023), [https://www.teletrust.de/fileadmin/user\\_upload/2023-05\\_TeleTrust\\_Guideline\\_State\\_of\\_the\\_art\\_in\\_IT\\_security\\_EN.pdf](https://www.teletrust.de/fileadmin/user_upload/2023-05_TeleTrust_Guideline_State_of_the_art_in_IT_security_EN.pdf)
- <sup>82</sup> GrantThornton, IT Security Act 2.0 & KRITIS Regulation 2023—challenges for mid-market companies to master, (October 26, 2023), <https://www.grantthornton.de/en/insights/2023/it-security-act-2-0-kritis-regulation-2023-challenges-for-mid-market-companies-to-master/>
- <sup>83</sup> Federal Council, Information Security Act, ISG, (January 1, 2024), [https://www.fedlex.admin.ch/eli/cc/2022/232/de#art\\_64](https://www.fedlex.admin.ch/eli/cc/2022/232/de#art_64)
- <sup>84</sup> Cyber and Infrastructure Security Centre, Critical Infrastructure Risk Management Program, (Accessed October 23, 2023), <https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-risk-management-program.pdf>
- <sup>85</sup> Australian Signals Directorate, Essential Eight Maturity Model, (November 2023) <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-changes>
- <sup>86</sup> NISC, The Guidance on Operations of Cybersecurity Measures of Government Agencies and Related Agencies, 2023 (Japanese), <https://www.nisc.go.jp/pdf/policy/general/guider6.pdf>
- <sup>87</sup> Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition (Accessed October 30, 2023), [https://www.csa.gov.sg/docs/default-source/legislation/ccop\\_second-edition.pdf?sfvrsn=b2ab666a\\_2](https://www.csa.gov.sg/docs/default-source/legislation/ccop_second-edition.pdf?sfvrsn=b2ab666a_2)
- <sup>88</sup> Cyber Safety Review Board, Review of the Attacks Associated with Lapsus\$ and Related Threat Groups, (July 24, 2023) [https://www.cisa.gov/sites/default/files/2023-08/CSRB\\_Lapsus%24\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf)
- <sup>89</sup> NIST, FIPS 201-3, (January 2022), <https://doi.org/10.6028/NIST.FIPS.201-3>
- <sup>90</sup> Russell T. Vought, M-19-17, (May 21, 2019), <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>
- <sup>91</sup> Margaret M. Weichert, M-20-19, (March 22, 2020), <https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-19.pdf>
- <sup>92</sup> NIST, FIPS 140-3, (March 2019), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>
- <sup>93</sup> The White House, Executive order on Improving the Nation’s Cybersecurity, (May 12, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- <sup>94</sup> Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
- <sup>95</sup> White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 2022), <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/?mod=djemCIO>
- <sup>96</sup> NIST, SP 800-207 Zero Trust Architecture, (August 2020), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- <sup>97</sup> OMB, M-21-30 Protecting Critical Software Through Enhanced Security Measures, (August 10, 2021), <https://whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf>
- <sup>98</sup> NIST, Security Measures for “EO-Critical Software” Use Under Executive Order (EO) 14028, (July 9, 2021), <https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf>
- <sup>99</sup> NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf>
- <sup>100</sup> NIST, NIST SP 800-217 Guidelines for Personal Identity Verification (PIV) Federation, (January 2023), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-217.ipd.pdf>
- <sup>101</sup> NIST, NIST SP 800-171r2, (February 2020), <https://doi.org/10.6028/NIST.SP.800-171r2>
- <sup>102</sup> NIST, SP 800-52-r5, (September 2020), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- <sup>103</sup> Department of Defense, Defense Federal Acquisition Regulation, (Accessed April 15, 2024), <https://www.acquisition.gov/sites/default/files/current/dfars/pdf/DFARS.pdf>
- <sup>104</sup> US Department of Defense, CMMC Program, (Accessed April 15, 2024), <https://dodcio.defense.gov/CMMC/About/>
- <sup>105</sup> NIST, SP 800-172 Enhanced SEcurity Requirements for Protecting Controlled Unclassified Information, (February 2021), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf>
- <sup>106</sup> Government of Canada, Directive on Service and Digital, (January 10, 2024), <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601>
- <sup>107</sup> NCSC, NCSC CAF guidance, (Accessed April 16, 2024), <https://www.ncsc.gov.uk/collection/cyber-assessment-framework>
- <sup>108</sup> National Cyber Security Centre, Cyber Essentials: Requirements for IT infrastructure v3.1, (April 2023), <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf>
- <sup>109</sup> NISC, Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies, (FY2021), <https://www.nisc.go.jp/eng/pdf/kijyunr3-en.pdf>
- <sup>110</sup> NISC, Guidelines for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition), (April 4, 2018), [https://www.nisc.go.jp/eng/pdf/principles\\_ci\\_eng\\_v5\\_r1.pdf](https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5_r1.pdf)
- <sup>111</sup> Australian Government, Privacy Act 1988, (Accessed April 16, 2024), <https://www.legislation.gov.au/C2004A03712/asmade/text>
- <sup>112</sup> PCI, PCI DSS: v4.0.1, (June 2024), [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\\_0\\_1.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf)
- <sup>113</sup> MAS, MAS’ Cyber Security Advisory Panel Proposes Ways to Tackle Mobile Malware Scams and Generative AI Risks for the Financial Sector, (October 30, 2023), [https://www.csa.gov.sg/docs/default-source/legislation/ccop\\_second-edition.pdf?sfvrsn=b2ab666a\\_2](https://www.csa.gov.sg/docs/default-source/legislation/ccop_second-edition.pdf?sfvrsn=b2ab666a_2)
- <sup>114</sup> CFPB, Consumer Financial Protection Circular 2022-04, (August 11, 2022), <https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/>

## Sources

- <sup>115</sup> PCI, PCI DSS: v4.0, (March 2022), [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\\_0.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf)
- <sup>116</sup> FTC, Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses, (October 27, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data>
- <sup>117</sup> FTC, Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses, (October 27, 2021), <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial>
- <sup>118</sup> FFIEC, Authentication and Access to Financial Institution Services and Systems Guidance, (August 11, 2021), <https://www.ffiec.gov/press/pr081121.htm>
- <sup>119</sup> FFIEC, Authentication and Access to Financial Institution Services and Systems, (August 11, 2021), <https://www.federalreserve.gov/supervisionreg/srletters/sr2114.pdf>
- <sup>120</sup> CFPB, Consumer Financial Protection Circular 2022-04 (August 11, 2022), <https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/>
- <sup>121</sup> SEC, Cybersecurity Risk Management, Strategy, Governance, and Incident Discloser, (September 5, 2023), <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>
- <sup>122</sup> EU, Directive 2015/2366, (25 November 2015), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>
- <sup>123</sup> DORA, Article 6 ICT Risk Management Framework, (Accessed April 16, 2024), <https://www.dora-info.eu/dora/article-6/>
- <sup>124</sup> European Commission, Digital Operational Resilience Act (Accessed April 10, 2024), [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)
- <sup>125</sup> David Jones, White House wants to set minimum cyber standards for hospitals, healthcare, (December 11, 2023), <https://www.cybersecuritydive.com/news/biden-minimum-cyber-standards-healthcare/702129/>
- <sup>126</sup> Enzoic, Recommendations for HIPAA Password Compliance, (March 23, 2020), <https://securityboulevard.com/2020/03/recommendations-for-hipaa-password-compliance/>
- <sup>127</sup> Congress, H.R. 7898, (January 5, 2021), <https://www.congress.gov/bill/116th-congress/house-bill/7898?s=1&r=2>
- <sup>128</sup> NIST, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, (February 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf>
- <sup>129</sup> US FDA, CFR - Code of Federal Regulations Title 21, (April 1, 2020), <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=1311.55>
- <sup>130</sup> US Department of Justice, Use of Mobile Devices in the Issuance of EPCS, (August 16, 2018), [https://www.deadversion.usdoj.gov/GDP/\(DEA-DC-8\)%20Use%20of%20Mobile%20Devices%20in%20the%20Issuance%20of%20EPCS.pdf](https://www.deadversion.usdoj.gov/GDP/(DEA-DC-8)%20Use%20of%20Mobile%20Devices%20in%20the%20Issuance%20of%20EPCS.pdf)
- <sup>131</sup> ONC, 21st Century Cures Act, (May 1, 2020), <https://www.federalregister.gov/documents/2023/11/01/2023-24068/21st-century-cures-act-establishment-of-disincentives-for-health-care-providers-that-have-committed>
- <sup>132</sup> White House, National Cybersecurity Strategy, (March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- <sup>133</sup> US Department of Energy, NARUC, Cybersecurity Baselines for Electric Distribution Systems and DER, (February 2024), <https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/>
- <sup>134</sup> UK Cabinet Office, National Cyber Strategy 2022, (December 15, 2022), <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#law-enforcements-national-cyber-crime-network>
- <sup>135</sup> KPMG, Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection, (2016), <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/Cyber-Security-Standards-Compliance-A-Vital-Measure-to-Critical-Infrastructure-Protection.pdf>
- <sup>136</sup> NERC, CIP-005-7, (Accessed October 23, 2023), <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-7.pdf>
- <sup>137</sup> DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021), <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>
- <sup>138</sup> TSA, Security Directive Pipeline-2021-01D (May 20, 2024), <https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf>
- <sup>139</sup> CISA, Multifactor Authentication, (Accessed April 16, 2024), <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>
- <sup>140</sup> TSA, Security Directive Pipeline-2021-02D, (July 26, 2023), [https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo\\_07\\_27\\_2023.pdf](https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf)
- <sup>141</sup> TSA, Security Directive 1580/82-2022-01, (October 24, 2022), <https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf>
- <sup>142</sup> TSA, TSA issues new cybersecurity requirements for airport and aircraft operators, (March 2023), <https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft>
- <sup>143</sup> EPA, Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process, (March 3, 2023), [https://www.epa.gov/system/files/documents/2023-10/addressing-pws-cybersecurity-in-sanitary-surveys-memo\\_march-2023.pdf](https://www.epa.gov/system/files/documents/2023-10/addressing-pws-cybersecurity-in-sanitary-surveys-memo_march-2023.pdf)
- <sup>144</sup> UK Legislation, Telecommunications (Security) Act 2021, (2021), <https://www.legislation.gov.uk/ukpga/2021/31/section/1/enacted>
- <sup>145</sup> European Commission, Annexes to the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, (Sept 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454>
- <sup>146</sup> AEMO, Australian Energy Sector Cyber Security Framework, (Accessed October 26, 2023), <https://aemo.com.au/en/initiatives/major-programs/cyber-security>
- <sup>147</sup> AEMO, AESCSF framework and resources (Accessed October 23, 2023), <https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources>
- <sup>148</sup> NACSA, CYBER SECURITY ACT 2024 (ACT 854) (Accessed September 25, 2024), <https://www.nacsa.gov.my/act854.php>
- <sup>149</sup> DOD OCIO, Memo, (December 20, 2019), <https://dodcio.defense.gov/Portals/0/Documents/Cyber/DODCIOMem-MobilePKICredentials.pdf>
- <sup>150</sup> Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022), <https://www.yubico.com/resource/tei-forrester-report/>
- <sup>151</sup> S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023 <https://www.yubico.com/resource/yubico-and-sp-global-market-intelligence-research-report/>



## About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: [www.yubico.com](https://www.yubico.com).