تاب‌آوری سایبری در صنایع

تیرماه 1404

تنها ۲ دسته سازمان وجود دارد:
آنهایی که هک شده‌اند و آنهایی که هک خواهند شد.

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

فهرست مباحث

1

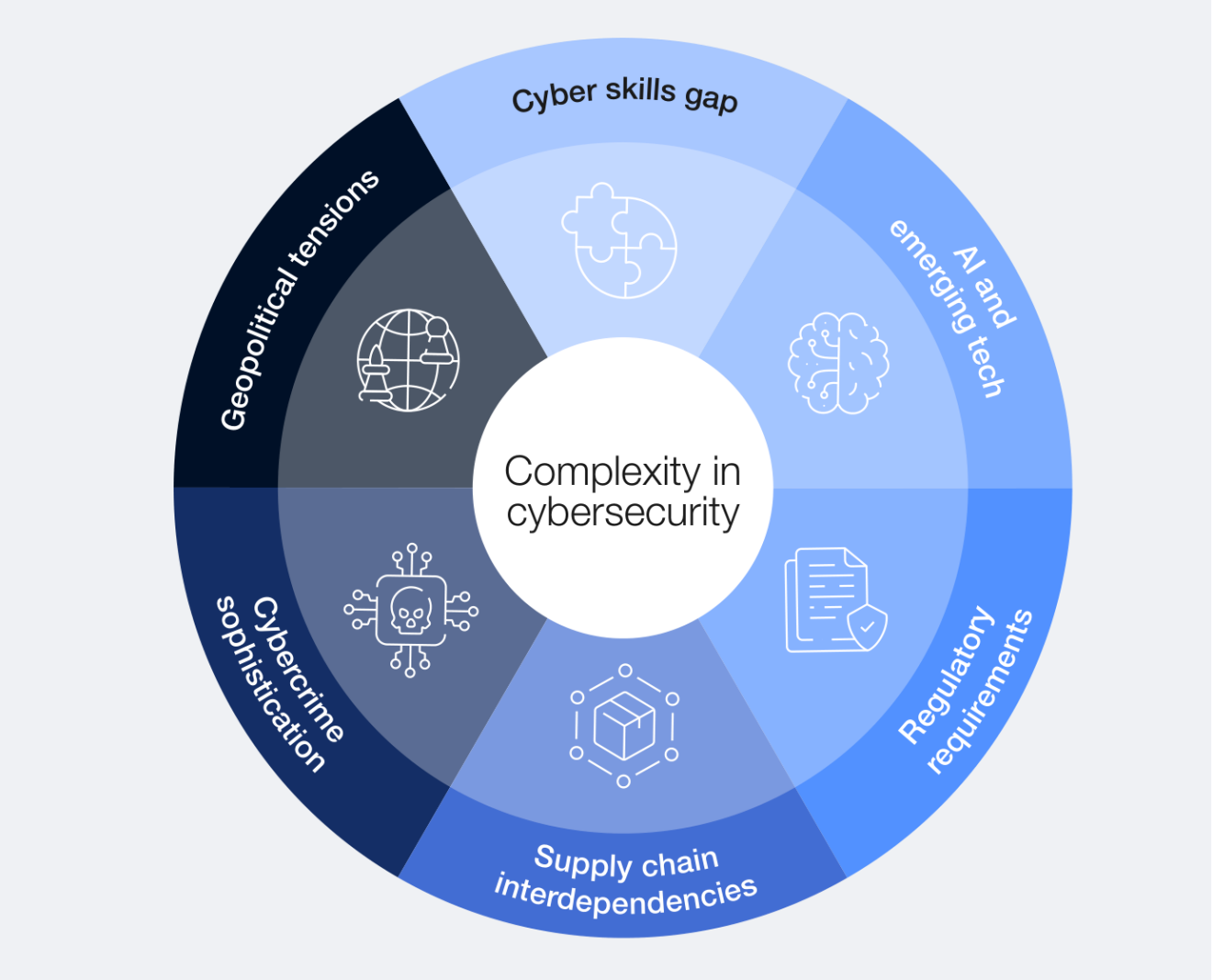
مقدمه

Executive summary

In a complex cyberspace characterized by geopolitical uncertainties, widening cyber inequity and sophisticated cyberthreats, leaders must adopt a security-first mindset.

- در فضای سایبری پیچیده‌ای که با عدم‌قطعیت‌های ژئوپلیتیکی، گسترش نابرابری سایبری و تهدیدات سایبری پیشرفته مشخص می‌شود، رهبران باید ذهنیت اولویت بخشی به امنیت را اتخاذ کنند.

عوامل موثر بر پیچیدگی امنیت سایبری



عوامل موثر بر پیچیدگی امنیت سایبری

وابستگی‌های متقابل زنجیره تأمین

با توجه به اینکه 54 درصد از سازمان‌های بزرگ، مدیریت ریسک شخص ثالث را به عنوان یک چالش اصلی ذکر می‌کنند، چالش‌های زنجیره تأمین همچنان نگرانی اصلی برای دستیابی به تاب‌آوری سایبری است

پیچیدگی جرایم سایبری

72 درصد از پاسخ‌دهندگان می‌گویند که خطرات سایبری در سال گذشته افزایش یافته است و کلاهبرداری سایبری، افزایش حملات فیشینگ و مهندسی اجتماعی و سرقت هویت به عنوان خطرات اصلی سایبری شخصی تبدیل شده‌اند.

تنش‌های ژئوپلیتیک

تنش‌های ژئوپلیتیک در تقریباً 60 درصد از سازمان‌ها بر استراتژی سایبری تأثیر می‌گذارند، به طوری که از هر سه مدیرعامل، یک نفر جاسوسی سایبری و از دست دادن اطلاعات حساس/IP را به عنوان نگرانی‌های اصلی خود ذکر می‌کند.

شکاف مهارت‌های سایبری

شکاف مهارت‌های سایبری از سال ۲۰۲۴ افزایش یافته است، به طوری که از هر سه سازمان، دو سازمان شکاف‌های مهارت‌های متوسط تا بحرانی را گزارش می‌کنند. تنها ۱۴٪ از سازمان‌ها مطمئن هستند که افراد و مهارت‌های مورد نیاز را دارند

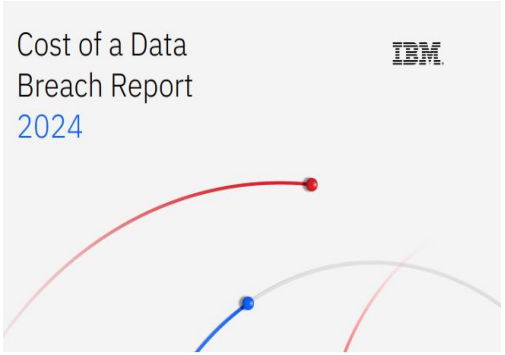
هوش مصنوعی و فناوری‌های نوظهور

66 درصد از پاسخ‌دهندگان معتقدند که هوش مصنوعی در 12 ماه آینده بر امنیت سایبری تأثیر خواهد گذاشت، اما تنها 37 درصد فرآیندهایی برای استقرار ایمن هوش مصنوعی دارند.

الزامات نظارتی

78 درصد از رهبران سازمان‌های خصوصی احساس می‌کنند که مقررات سایبری و حریم خصوصی به طور مؤثر ریسک را در اکوسیستم‌های سازمان آنها کاهش می‌دهد. با این حال، دو سوم از پاسخ‌دهندگان، پیچیدگی و گسترش الزامات نظارتی را به عنوان یک چالش ذکر کردند.

گزارش‌های مورد استفاده



تاب‌آوری سایبری

- تعریف تاب‌آوری سایبری (Cyber Resilience)

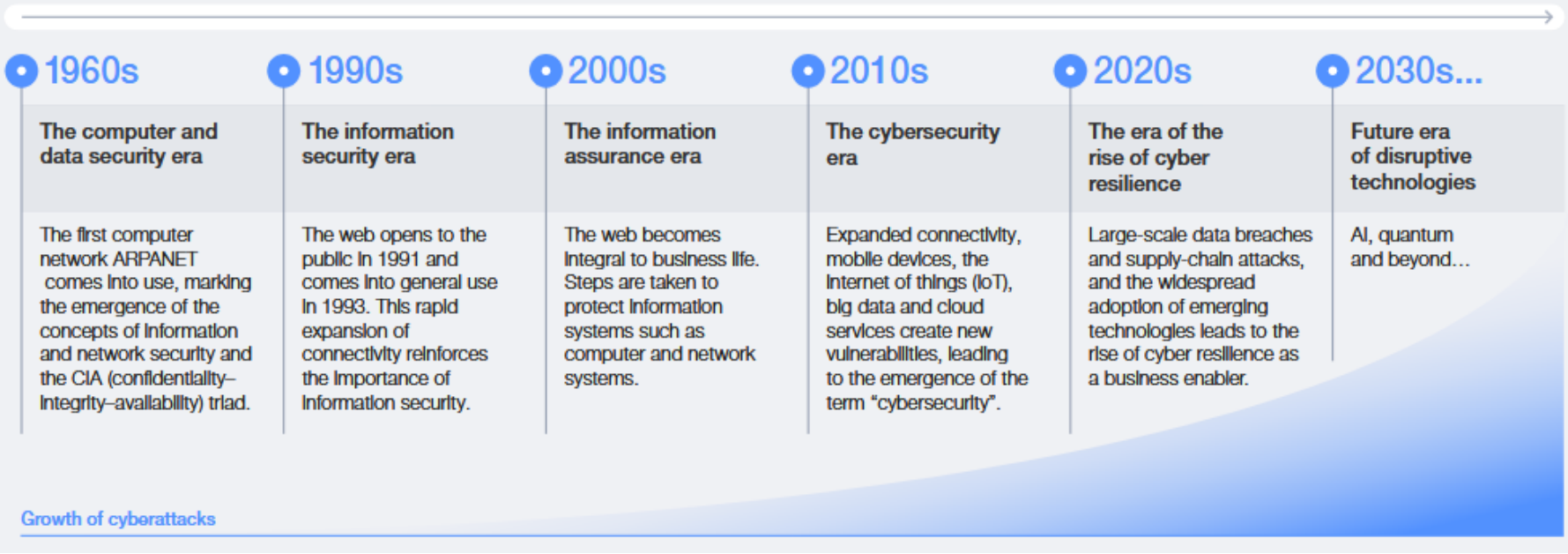
- توانایی یک نهاد در ارائه مستمر نتایج و دستاوردهای مورد نظر، علیرغم حملات سایبری.

امنیت سایبری: ضرورت استراتژیک

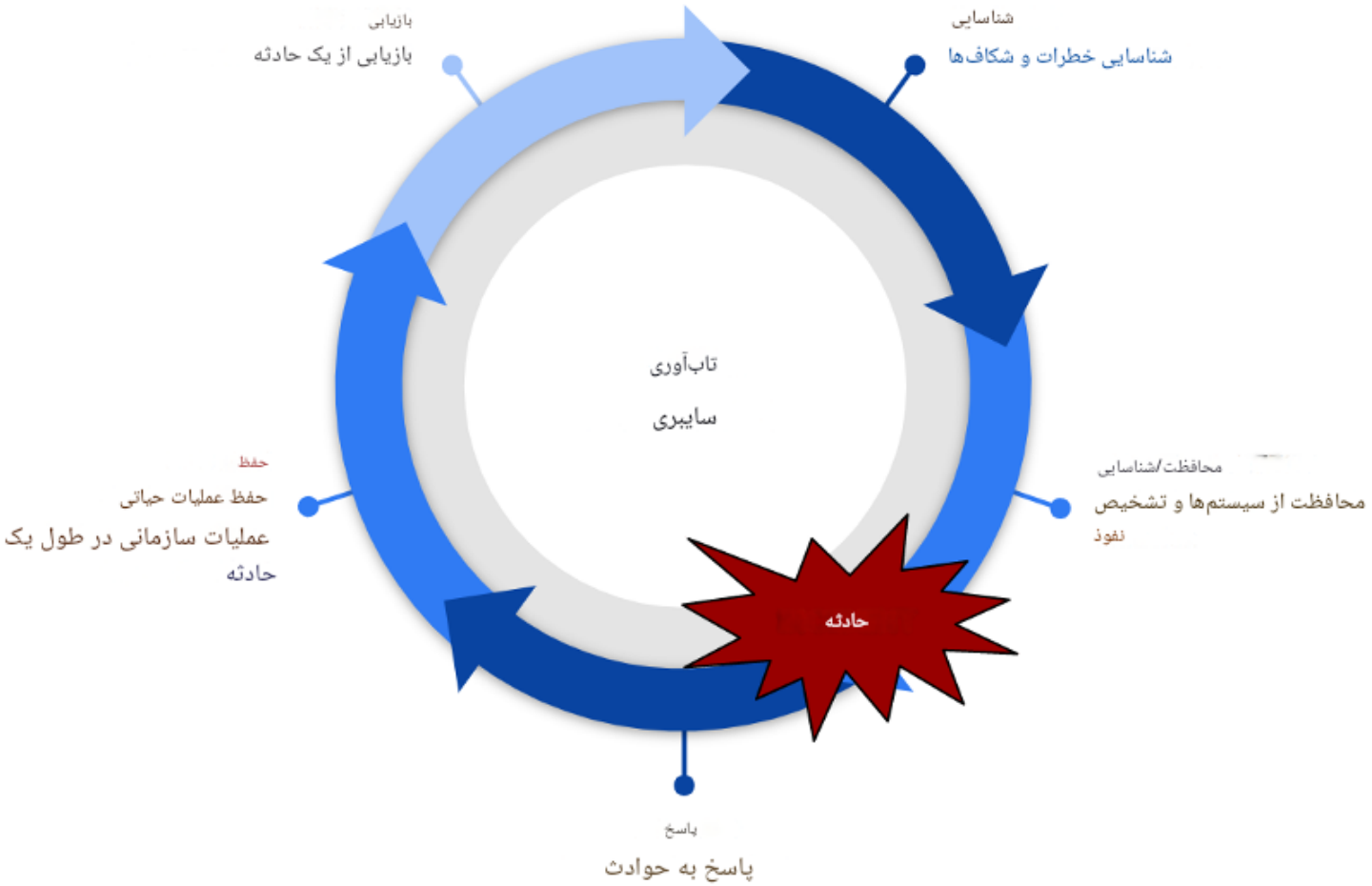
- Achieving true cyber resilience is fundamentally a leadership issue.
- دستیابی به تاب‌آوری سایبری واقعی اساساً یک مسئله رهبری است.
- برای موفقیت در عصر دیجیتال، سازمان‌ها باید تاب‌آوری سایبری را به‌عنوان یک موضوع راهبردی در رهبری در اولویت قرار دهند تا بتوانند اهداف اصلی کسب‌وکار را محافظت کرده و رشد بلندمدت را حفظ کنند.

از امنیت سایبری تا تاب آوری سایبری

FIGURE 1 | The evolution from information security to cyber resilience

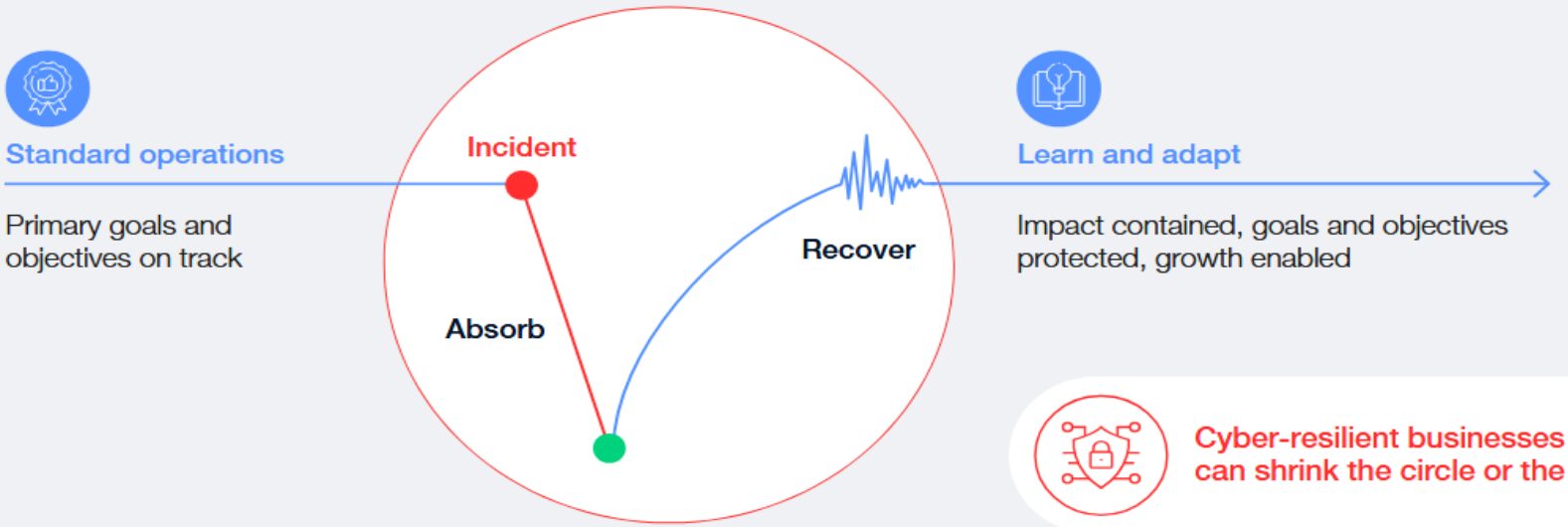


تاب آوری سایبری



تاب آوری سایبری

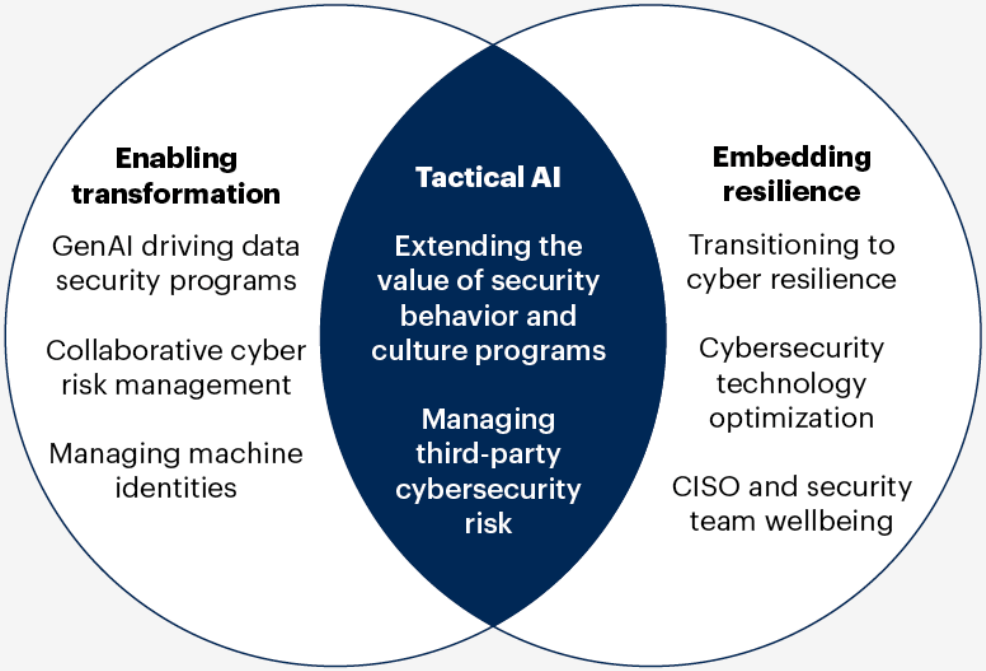
FIGURE 2 | **Organizations resilient to cyber incidents minimize the impact on primary goals and objectives**



Source: Adapted by the World Economic Forum and the University of Oxford from Linkov, I., & Trump, B.D. (2019). *The science and practice of resilience: Risk, systems and decisions*, Chapter 6. Springer. https://doi.org/10.1007/978-3-030-04565-4_6

روندهای برتر امنیت سایبری در سال 2025

Top Trends in Cybersecurity for 2025



Source: Gartner

Gartner

روندهای برتر امنیت سایبری در سال 2025

اهمیت اثر حملات بر کسب و کارها

کدام کسب و کارها هدف حملات سایبری اند؟

60%

of small and medium-sized businesses are likely to go out of business within six months of a cyberattack

47%

of small businesses say they have no understanding of how to protect themselves against cyberattacks

70%

of cyber attackers deliberately target small business

https://umbrella.cisco.com/blog/cybersecurity-for-small-business

اهمیت اثر حملات بر کسب و کارها

کدام کسب و کارها هدف حملات سایبری اند؟

۷۰٪ از

مهاجمان سایبری عمداً کسب‌وکارهای کوچک را هدف قرار می‌دهند

۴۷٪

از کسب‌وکارهای کوچک می‌گویند که هیچ درکی از نحوه محافظت از خود در برابر حملات سایبری ندارند.

۶۰٪ از

کسب‌وکارهای کوچک و متوسط احتمالاً ظرف شش ماه پس از حمله سایبری ورشکست می‌شوند.

https://umbrella.cisco.com/blog/cybersecurity-for-small-business

امنیت سایبری: ضرورت استراتژیک

امنیت سایبری: ضرورت استراتژیک

زمان فرار (Breakout Time)

مدت زمانی که یک مهاجم برای شروع حرکت جانبی در شبکه شما نیاز دارد، در سال گذشته به پایین‌ترین سطح خود رسید:

کاهش میانگین آن به 48 دقیقه (کمتر از یک ساعت)
سریع‌ترین زمان فرار مشاهده‌شده تنها 51 ثانیه!!!

افزایش سرعت حملات سایبری و چالش‌های جدید برای تشخیص و مهار آن‌ها در زمان محدود است.

در سال 2024، هوش مصنوعی مولد (GenAI) نقشی محوری در کمپین‌های پیچیده حملات سایبری ایفا کرد.

این فناوری به مهاجمان امکان تولید ایمیل‌های فیشینگ هدفمند، محتوای متقاعدکننده و عمیق‌جعلی (مانند ویدئو و صدا) را داد و سطح پیچیدگی حملات را افزایش داد.

Average eCrime breakout time dropped to **48 minutes**, with the fastest breakout observed at just **51 seconds**

79% of detections in 2024 were malware-free, up from **40%** in 2019

Vishing attacks skyrocketed **442%** between the first and second half of 2024

52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access

چشم انداز امنیت سایبری

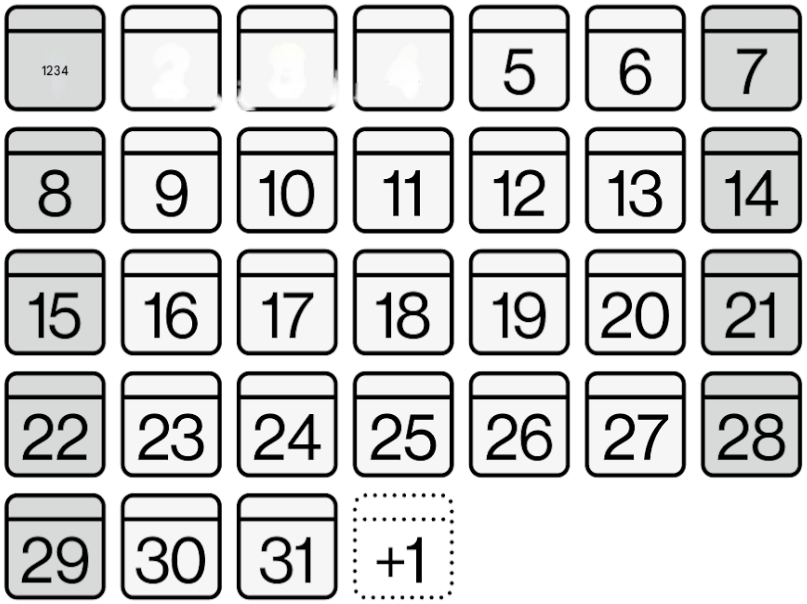
verizon
business

2025 Data Breach Investigations REPORT

چشم انداز امنیت سایبری

مجرمان سایبری امیدوارند که شما خیلی کند پاسخ دهید

یا کاملا از پاسخ دادن طفره بروید.



۳۲ روز

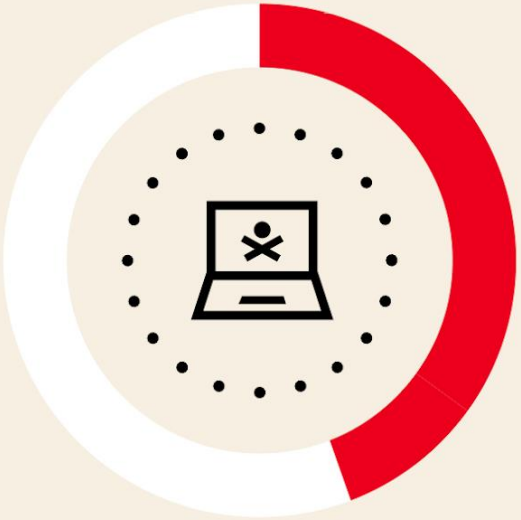
تحقیقات ما نشان می‌دهد که تنها حدود ٪۵۴ از آسیب پذیری های دستگاه های پیرامونی کاملا برطرف شده اند و انجام این کار به طور متوسط ۳۲ روز طول کشیده است.

چشم انداز امنیت سایبری

سازمان‌های بیشتری به گروگان گرفته می‌شوند.

۴۴

درصد از نقضهای امنیت سایبری مربوط به باج افزار بوده که نسبت به سال قبل ۳۷ درصد افزایش یافته است.

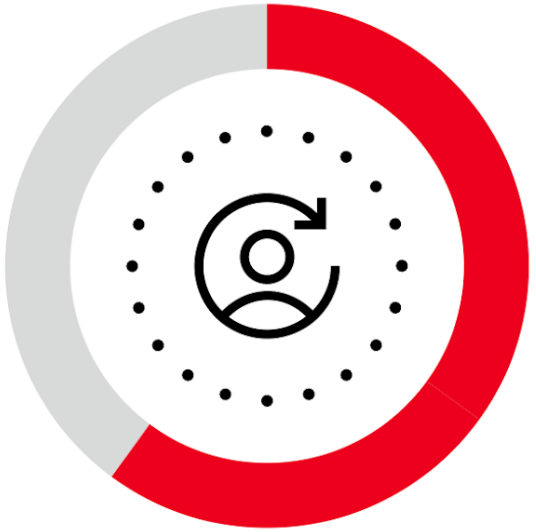


چشم انداز امنیت سایبری

عامل مشترک در بیشتر نقضهای داده ها چیست؟

"عامل انسانی"

۶۰ درصد



دخالت عامل انسانی در نقضهای امنیت سایبری تقریبا مانند سال قبل، تغییری نکرده است.

امنیت سایبری: ضرورت استراتژیک

چشم انداز تهدید 2024

در گزارش اولیه نظرسنجی خود در سال 2022، تهدیدات باج‌افزاری یکی از اولویت‌های اصلی بود.

باج‌افزار و سایر حملات سایبری تهدیدی واقعی برای کسب‌وکارها در سراسر جهان هستند.

چشم‌انداز تهدیدات در حال بدتر شدن است.

اثرات حملات سایبری در حوزه های مختلف صنعتی

پرداخت باج های سرسام آور

پرداخت باج بر خلاف سیاست
“do not pay”

چشم انداز تهدید 2024

احساس خوب نسبت به برنامه‌ریزی‌ها روی کاغذ یک موضوع است، اما توسعه و بهبود قابلیت‌ها برای اطمینان از اجرای موفقیت‌آمیز استراتژی برنامه‌ریزی‌شده، موضوعی دیگر است.

چشم انداز امنیت سایبری

امنیت سایبری: ضرورت استراتژیک

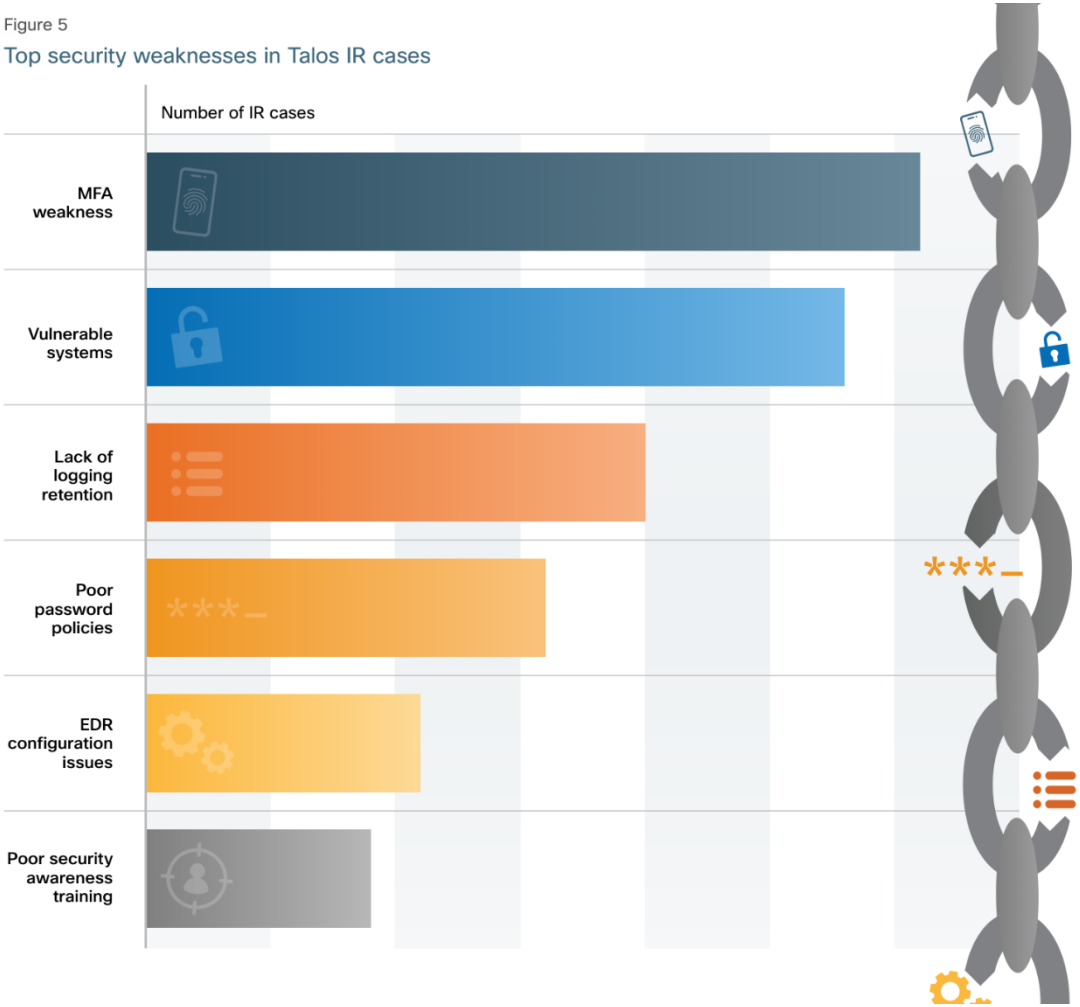
Figure 4

Top 10 most targeted network device vulnerabilities

Denotes EOL product

CVE	Manufacturer	Product	Device type	Vulnerability description
CVE-2024-24919	Check Point	Quantum Security Gateways	Firewall/VPN	Attacker can read sensitive data like password hashes.
CVE-2024-3273	D-Link	Multiple NAS Devices	Network attached storage (NAS)	Allows attacker to execute arbitrary base 64-encoded commands on the devices.
CVE-2024-3272	D-Link	Multiple NAS Devices	Network attached storage (NAS)	Allows attacker to execute arbitrary base 64-encoded commands on the devices.
CVE-2023-1389	TP-Link	Archer AX21	Router	Attacker can inject commands, which would be run as root, with a simple POST request.
CVE-2024-3400	Palo Alto Networks	PAN-OS	Firewall	Gives attacker ability to execute commands with root privileges on the firewall.
CVE-2023-36845	Juniper	Junos OS	Network device software	Attacker can inject and execute malicious code.
CVE-2021-44529	Ivanti	Endpoint Manager Cloud Service Appliance	Endpoint device manager	Allows attacker to execute malicious code with limited permissions.
CVE-2023-38035	Ivanti	Ivanti Sentry	Security gateway	Allows attacker to access sensitive API data and configurations, run system commands, or write files onto the system.
CVE-2024-36401	OSGeo	GeoServer	Server	Attacker can conduct remote code execution via specially crafted input.
CVE-2024-0012	Palo Alto Networks	PAN-OS	Firewall	Allows attacker to gain administrator privileges.

امنیت سایبری: ضرورت استراتژیک



امنیت سایبری: ضرورت استراتژیک

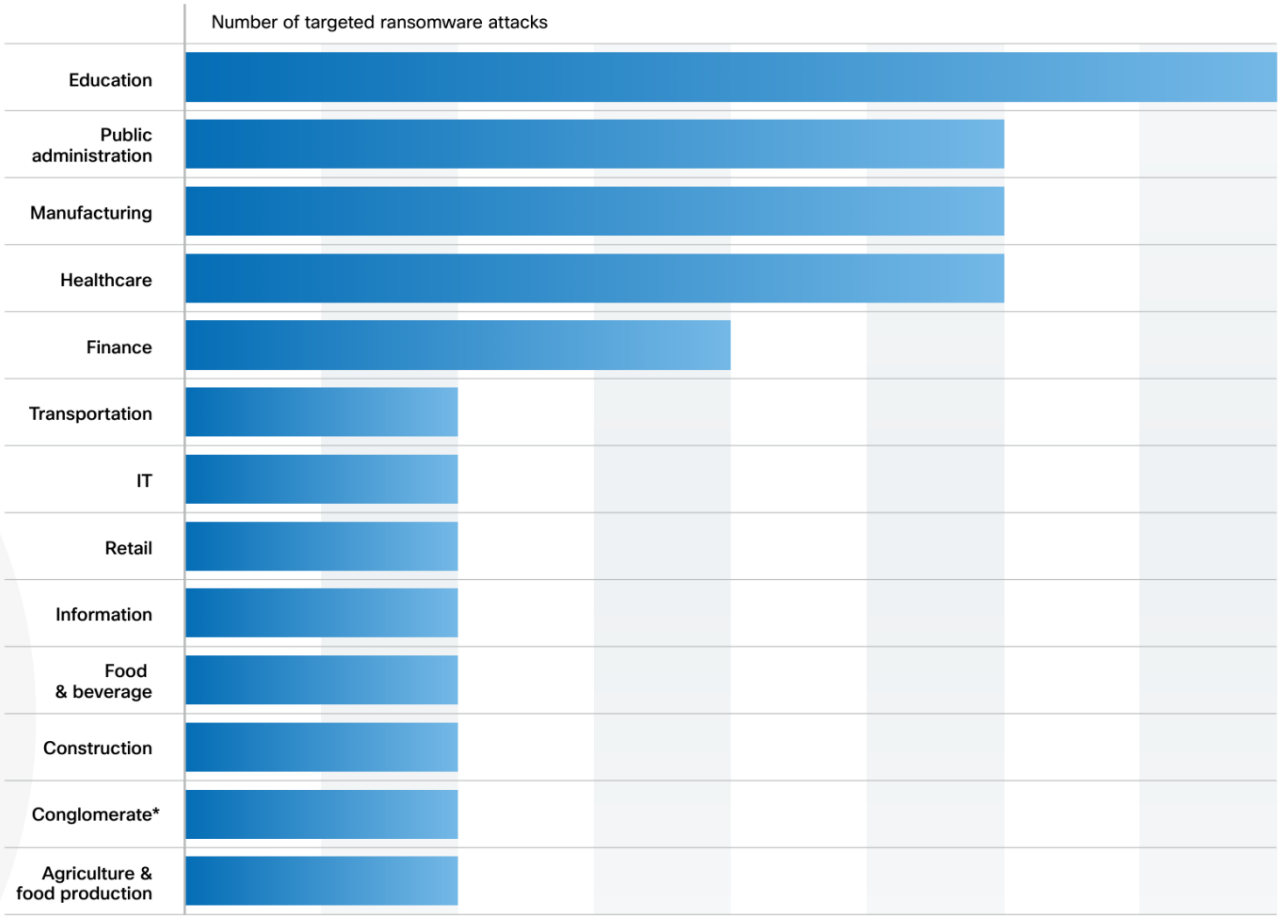
Talos' top 10 tips for securing network devices:

1. Update devices as aggressively as possible. This includes patching current hardware and software against known vulnerabilities and replacing EOL hardware and software.
2. Implement robust authentication methods. Use multifactor authentication, select complex passwords and community strings, and avoid default credentials.
3. Adhere to security best practices, including conducting regular updates, managing access controls, implementing user education, and enforcing network segmentation.
4. Encrypt all monitoring and configuration traffic, including SNMPv3, HTTPS, SSH, NETCONF, and RESTCONF.
5. Stay informed and up-to-date on security advisories from the U.S. government and industry. Consider suggested configuration changes to mitigate issues captured by these reports.
6. Lock down and actively monitor credential systems, such as TACACS+ and any jump hosts.
7. Store configurations centrally and push to devices. Do not allow devices to be the trusted source for their configurations.
8. Use authentication, authorization, and accounting (AAA) to deny configuration changes for key device protections, such as local accounts, TACACS+, and RADIUS.
9. Monitor your environment for unusual changes in behavior or configuration. Be on the lookout for exposure of administrative or unusual interfaces (such as SNMP, SSH, and HTTP(S)), and monitor syslog and AAA for unusual activities.
10. Profile your devices' baseline to identify any changes. Fingerprint network devices via NetFlow and port scanning for a shift in surface view, including new ports opening/closing and traffic to/from. When possible, develop NetFlow visibility to identify unusual volumetric changes.

امنیت سایبری: ضرورت استراتژیک

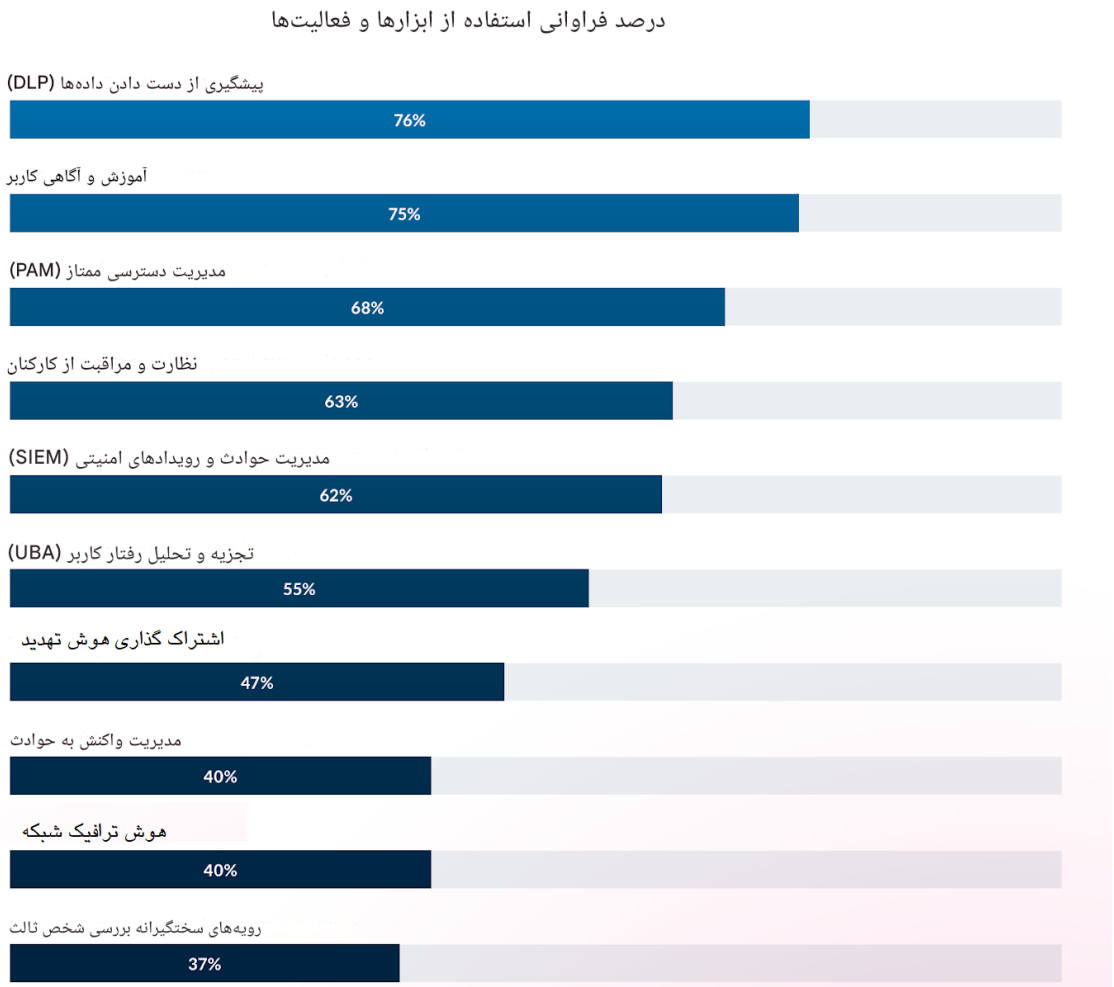
Figure 12

Targeted sectors

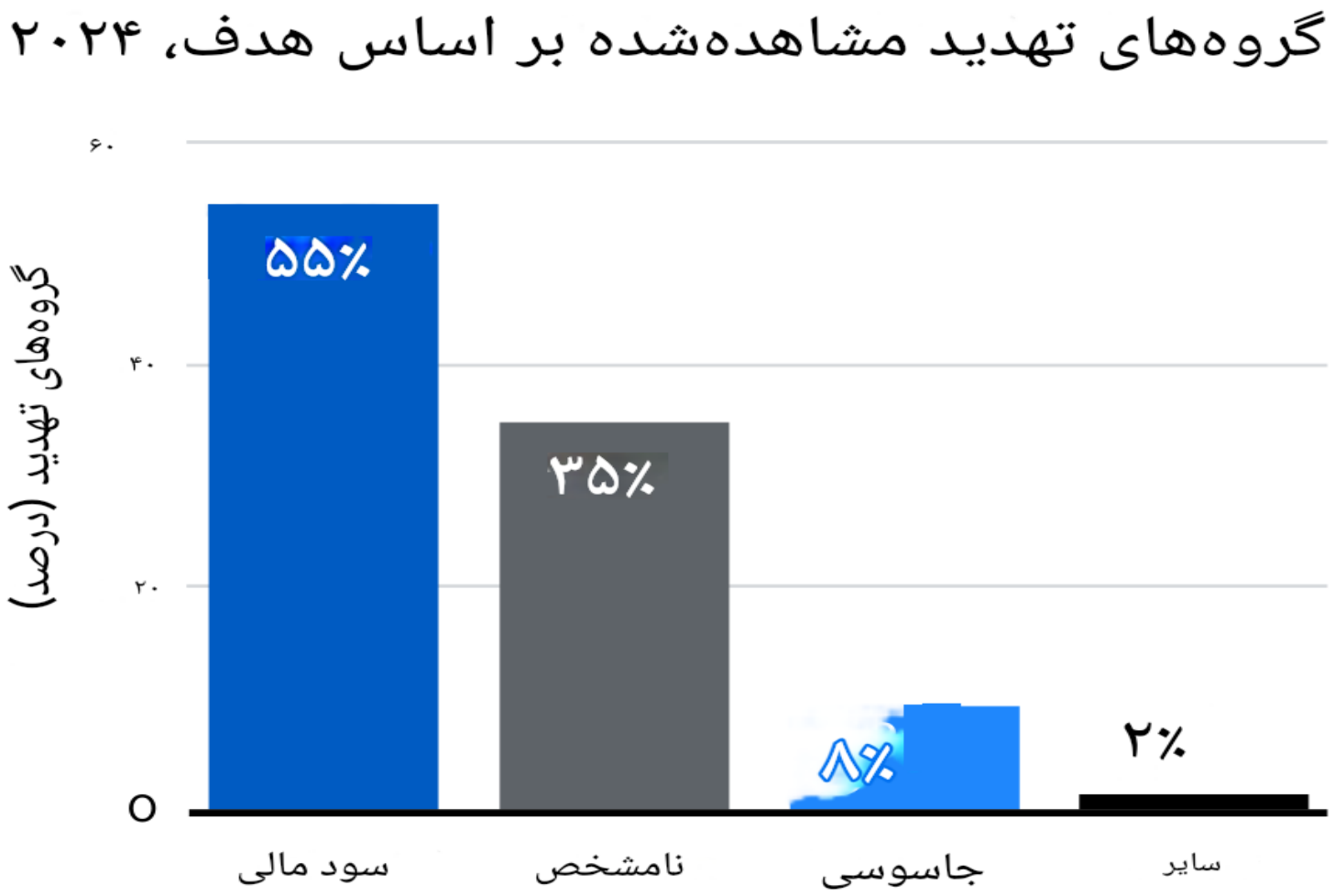


*Conglomerate organizations and their subsidiaries are not included in any other verticals.

امنیت سایبری: ضرورت استراتژیک



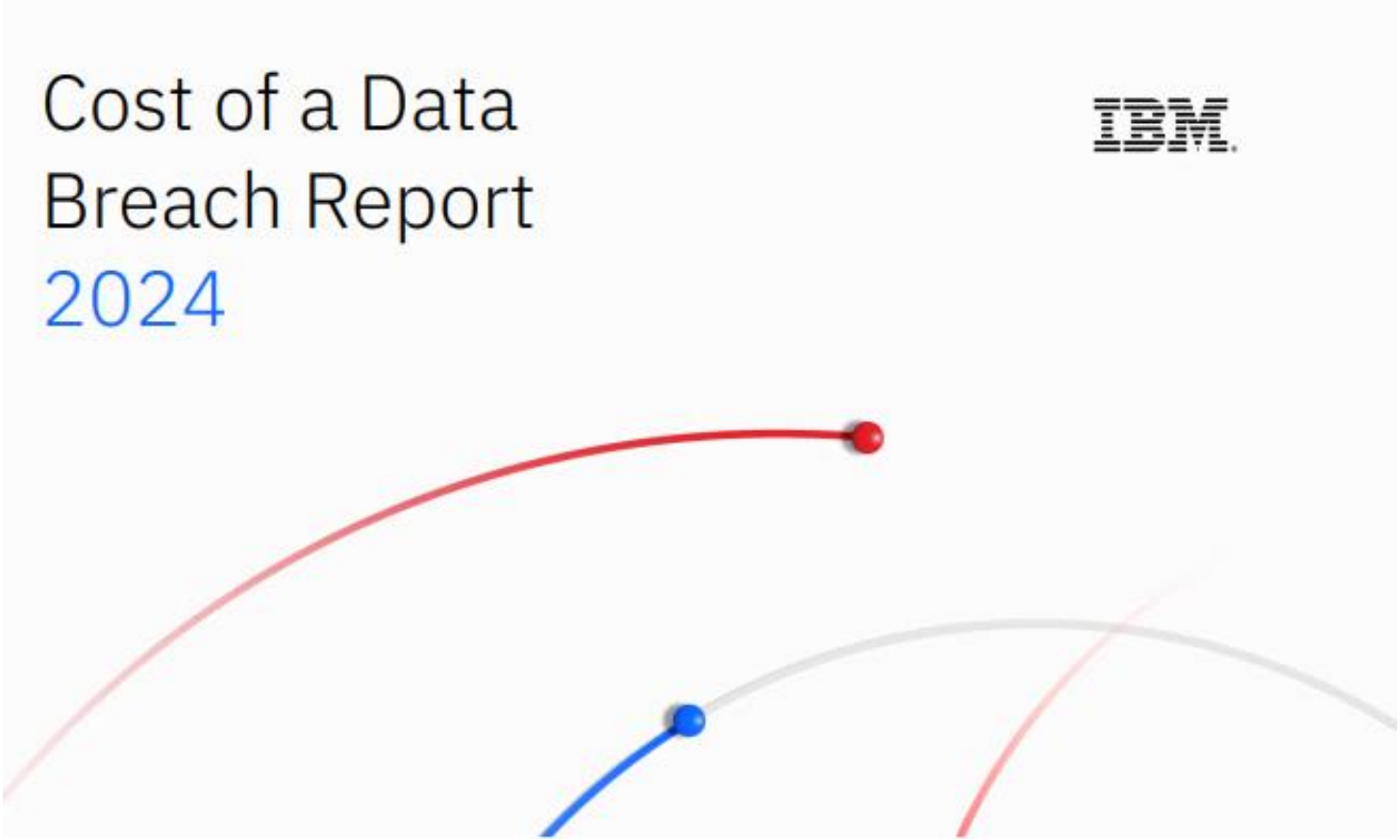
اهداف مجرمان سایبری



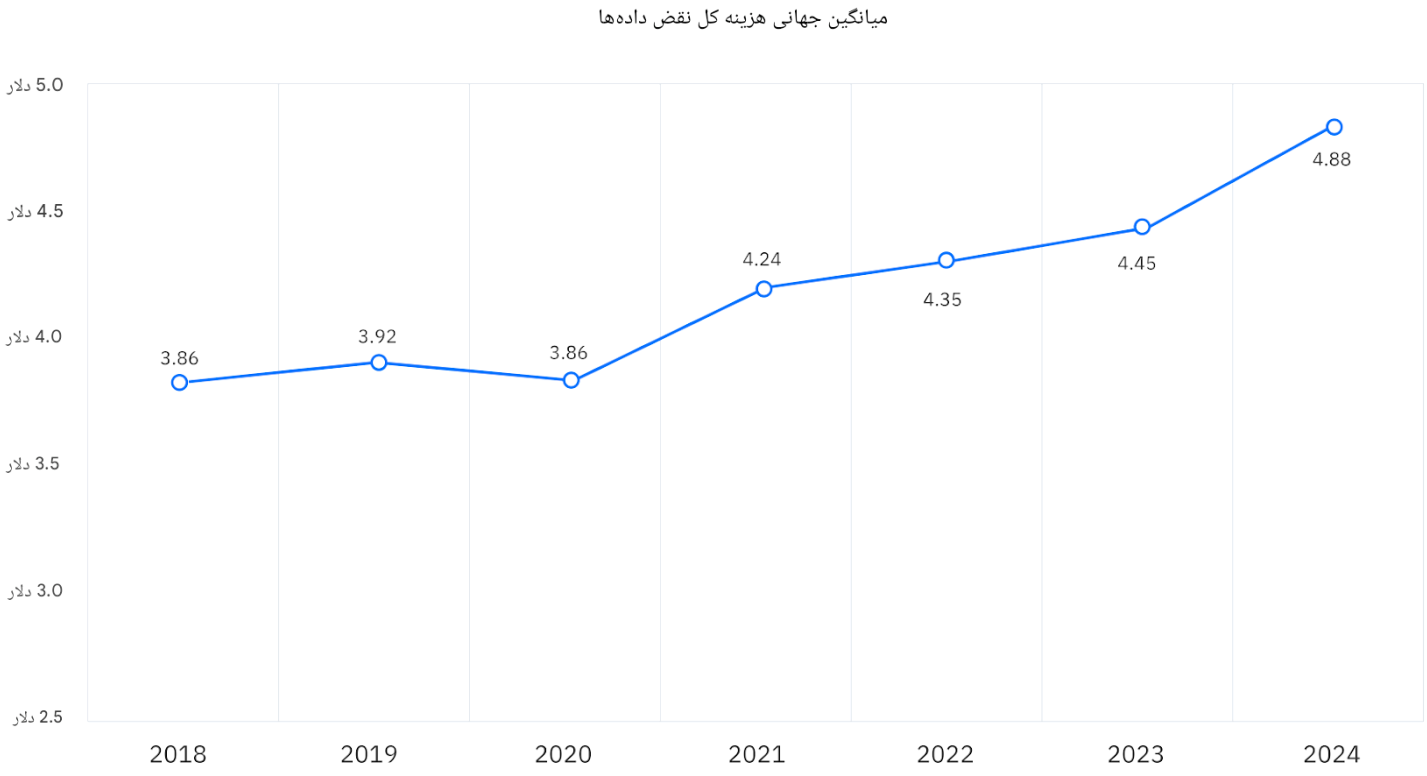
3

پیامدها و هزینه‌های رخدادهای سایبری و نشت داده

چشم انداز امنیت سایبری



چشم انداز امنیت سایبری



شکل 1. اندازه‌گیری شده به میلیون دلار آمریکا

گزارش هزینه نقض داده‌ها در سال 2024

چشم انداز امنیت سایبری

هزینه نقض داده‌ها بر اساس کشور یا منطقه

شماره	کشور	2024	2023
1	ایالات متحده	9.36 دلار	9.48 دلار
2	خاورمیانه	8.75 دلار	8.07 دلار
3	بنلوکس	5.90 دلار	—
4	آلمان	5.31 دلار	4.67 دلار
5	ایتالیا	4.73 دلار	3.86 دلار
6	کانادا	4.66 دلار	5.13 دلار
7	بریتانیا	4.53 دلار	4.21 دلار
8	ژاپن	4.19 دلار	4.52 دلار
9	فرانسه	4.17 دلار	4.08 دلار
10	آمریکای لاتین	4.16 دلار	3.69 دلار
11	کره جنوبی	3.62 دلار	3.48 دلار
12	اسه‌آن	3.23 دلار	3.05 دلار
13	استرالیا	2.78 دلار	2.70 دلار
14	آفریقای جنوبی	2.78 دلار	2.79 دلار
15	هند	2.35 دلار	2.18 دلار
16	برزیل	1.36 دلار	1.22 دلار

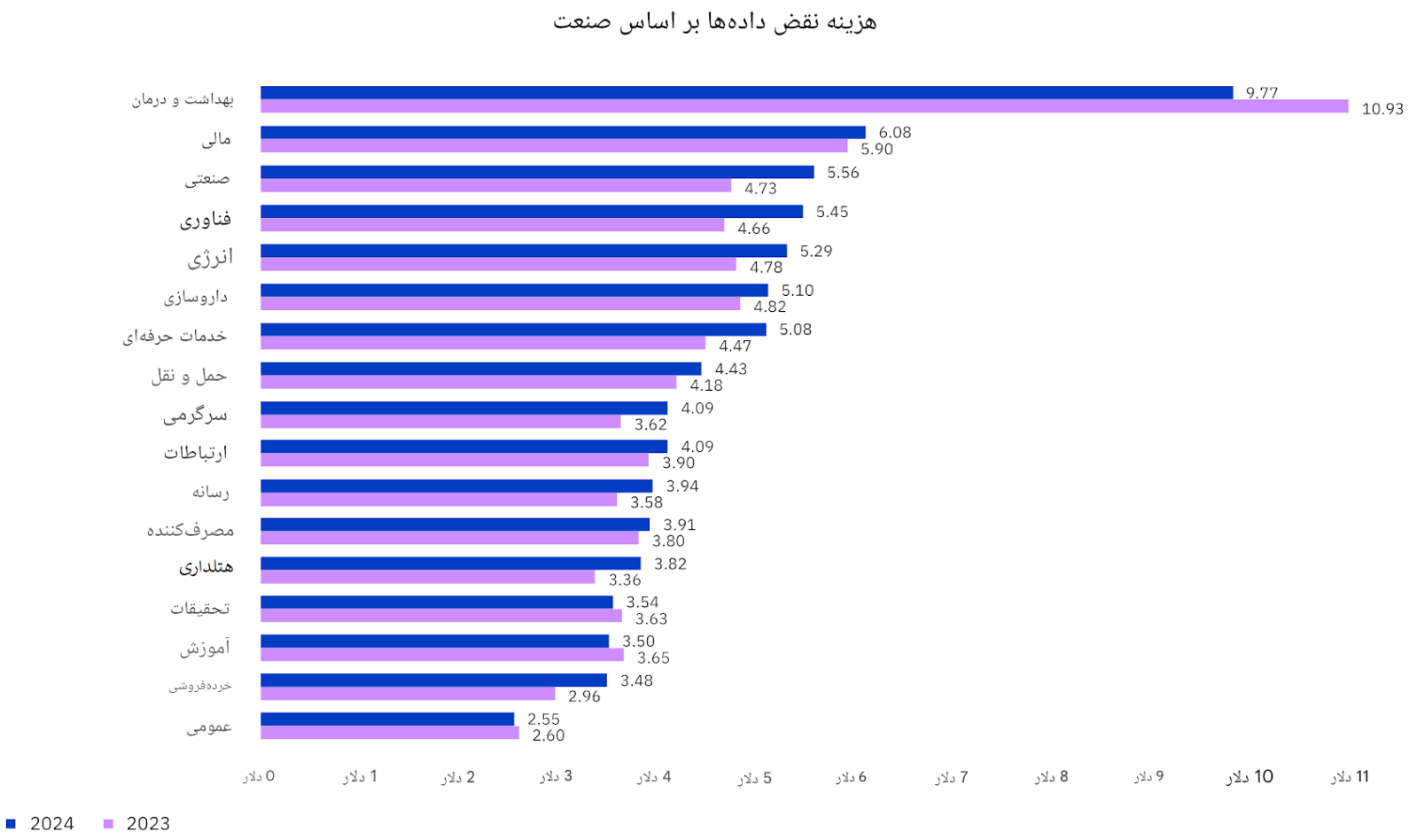
اندازه‌گیری شده به میلیون دلار آمریکا

5 کشور و منطقه برتر 2024 در مقابل 2023

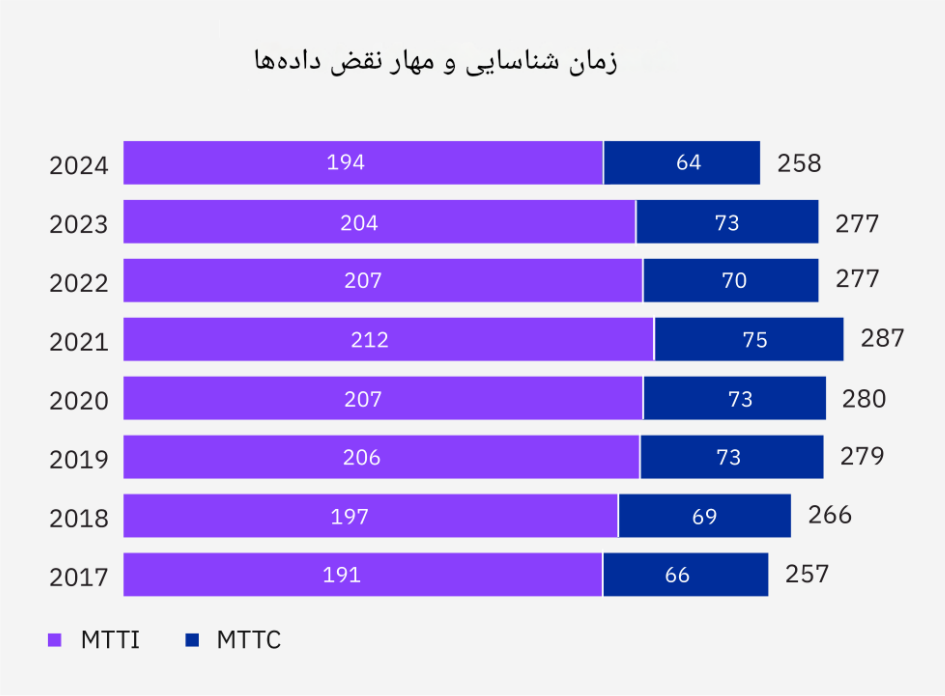
شماره	تغییر هزینه	2024	2023
1	↓	ایالات متحده 9.36 دلار	ایالات متحده 9.48 دلار
2	↑	خاورمیانه 8.75 دلار	خاورمیانه 8.07 دلار
3	↑	بنلوکس 5.90 دلار	کانادا 5.13 دلار
4	↑	آلمان 5.31 دلار	آلمان 4.67 دلار
5	↑	ایتالیا 4.73 دلار	ژاپن 4.52 دلار

اندازه‌گیری شده بر حسب میلیون دلار آمریکا

چشم انداز امنیت سایبری در صنایع مختلف



چشم انداز امنیت سایبری



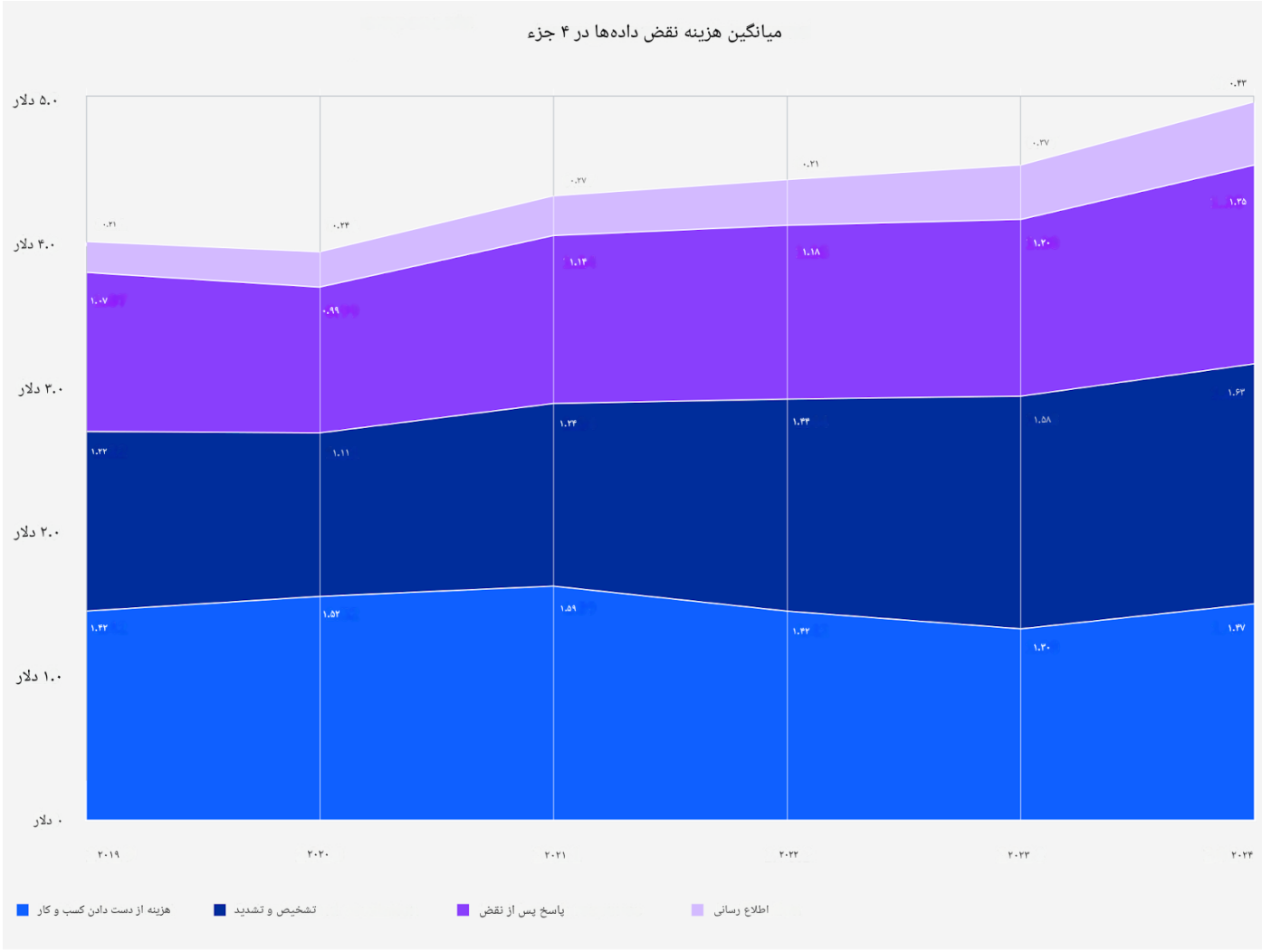
اندازه‌گیری شده بر حسب روز

در سال 2024 میانگین زمان شناسایی و مهار نقض داده کاهش یافت.

میانگین زمانی که مدافعان برای شناسایی و مهار یک نقض صرف کردند.

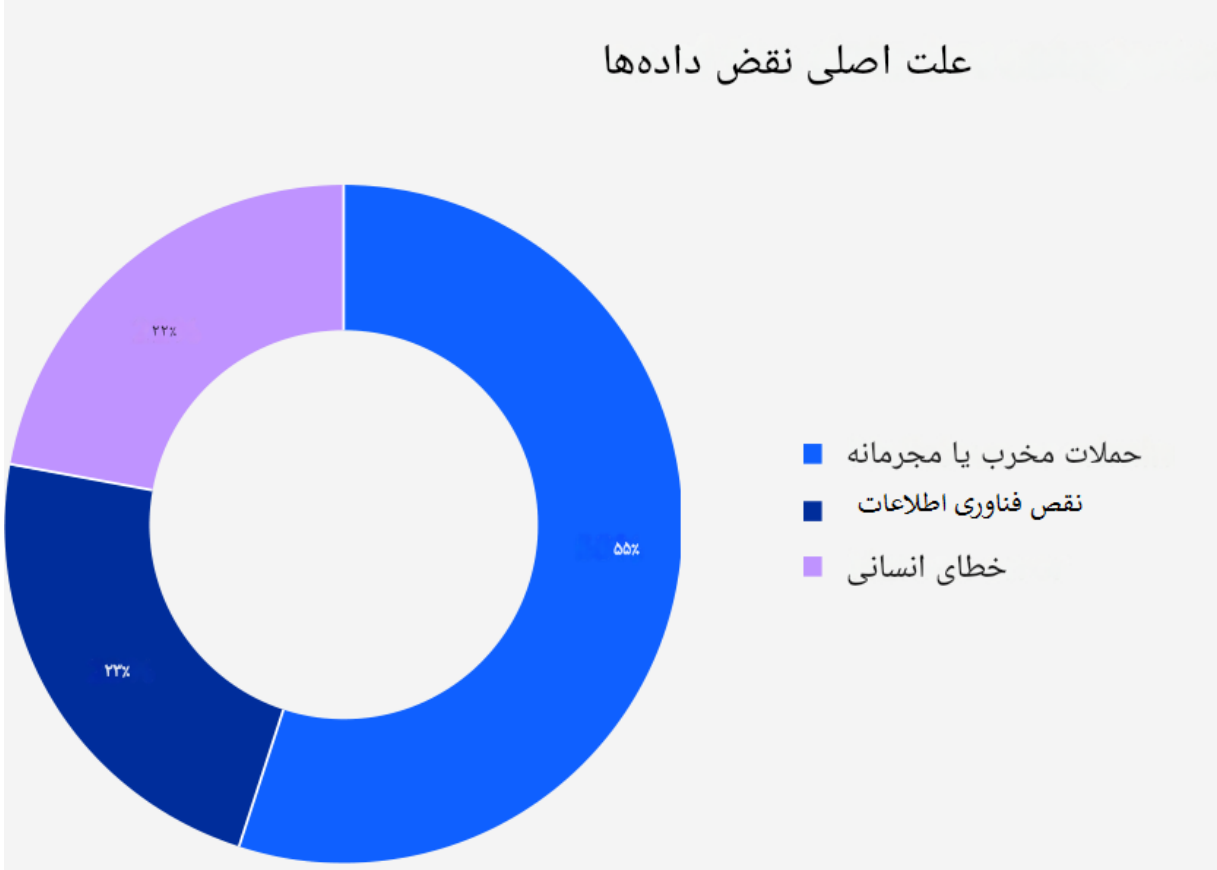
به 258 روز کاهش یافت و به پایین‌ترین سطح در هفت سال گذشته رسید، در مقایسه با 277 روز در سال قبل.

چشم انداز امنیت سایبری



شکل ۵. اندازه‌گیری شده بر حسب میلیون دلار آمریک

چشم انداز امنیت سایبری



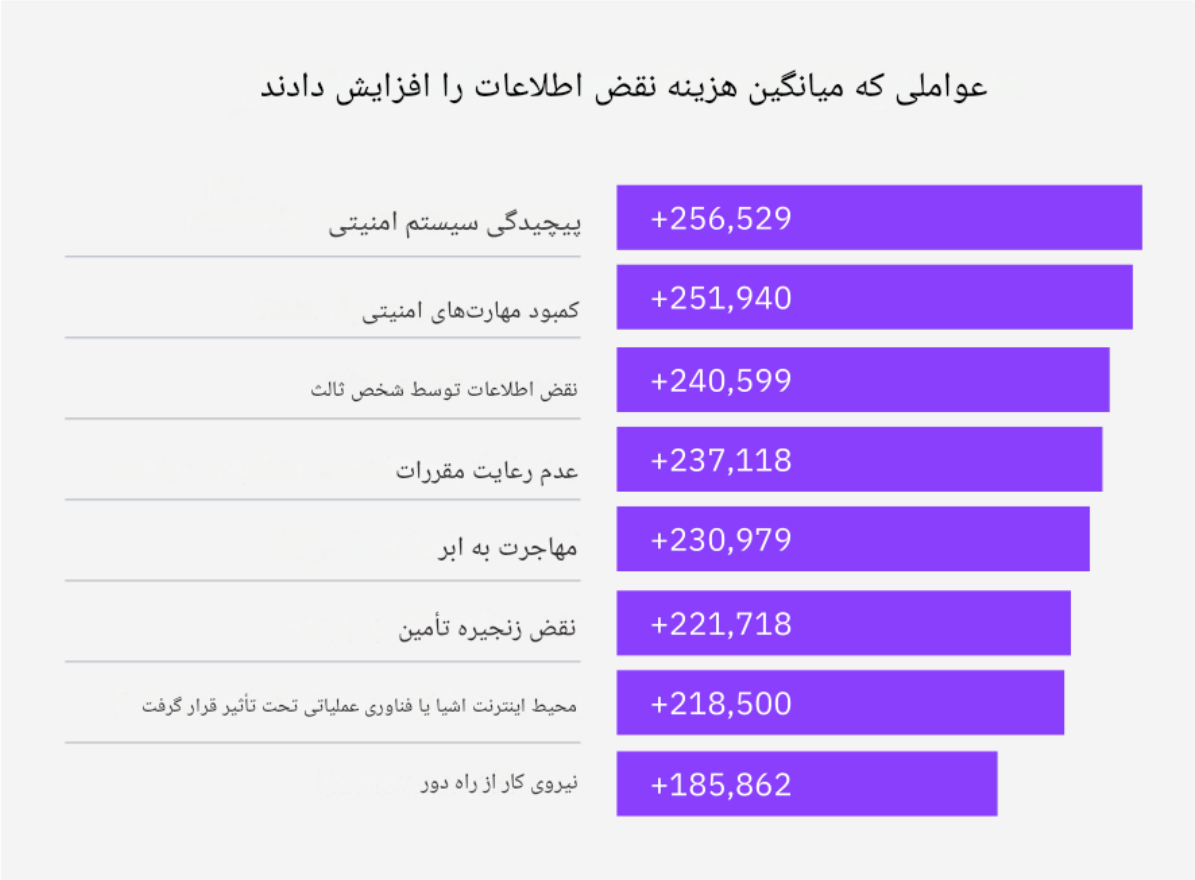
عوامل کلیدی کاهنده هزینه های نقض داده

آموزش کارکنان همچنان یک عنصر اساسی در استراتژی های دفاع سایبری به ویژه برای تشخیص و توقف حملات فیشینگ است.

بینشهای هوش مصنوعی و یادگیری ماشین با فاصله کمی در جایگاه دوم قرار گرفتند.

تفاوت هزینه از میانگین نقض ۴.۸۸ میلیون دلار آمریکا؛ اندازه‌گیری شده بر حسب دلار امریکا

امنیت سایبری: ضرورت استراتژیک



تفاوت هزینه از میانگین نقض اطلاعات 4.88 میلیون دلار
اندازه‌گیری شده بر حسب دلار آمریکا

مثالهای جهانی از تبعات رخدادهای سایبری

بهداشت و درمان

حمله باج‌افزاری به Universal Health Services (UHS) در 27 سپتامبر 2020، باعث اختلال در سیستم‌های بیمارستانی آمریکا و خسارت 67 میلیون دلاری شد.

NIST, Cybersecurity Case Studies: UHS, NISTIR 8272, 2022

تولید

حمله باج‌افزاری به Norsk Hydro در 19 مارس 2019،(باعث توقف تولید و خسارت 71 میلیون دلاری (52 میلیون دلار عملیاتی، 19 میلیون دلار مستقیم)

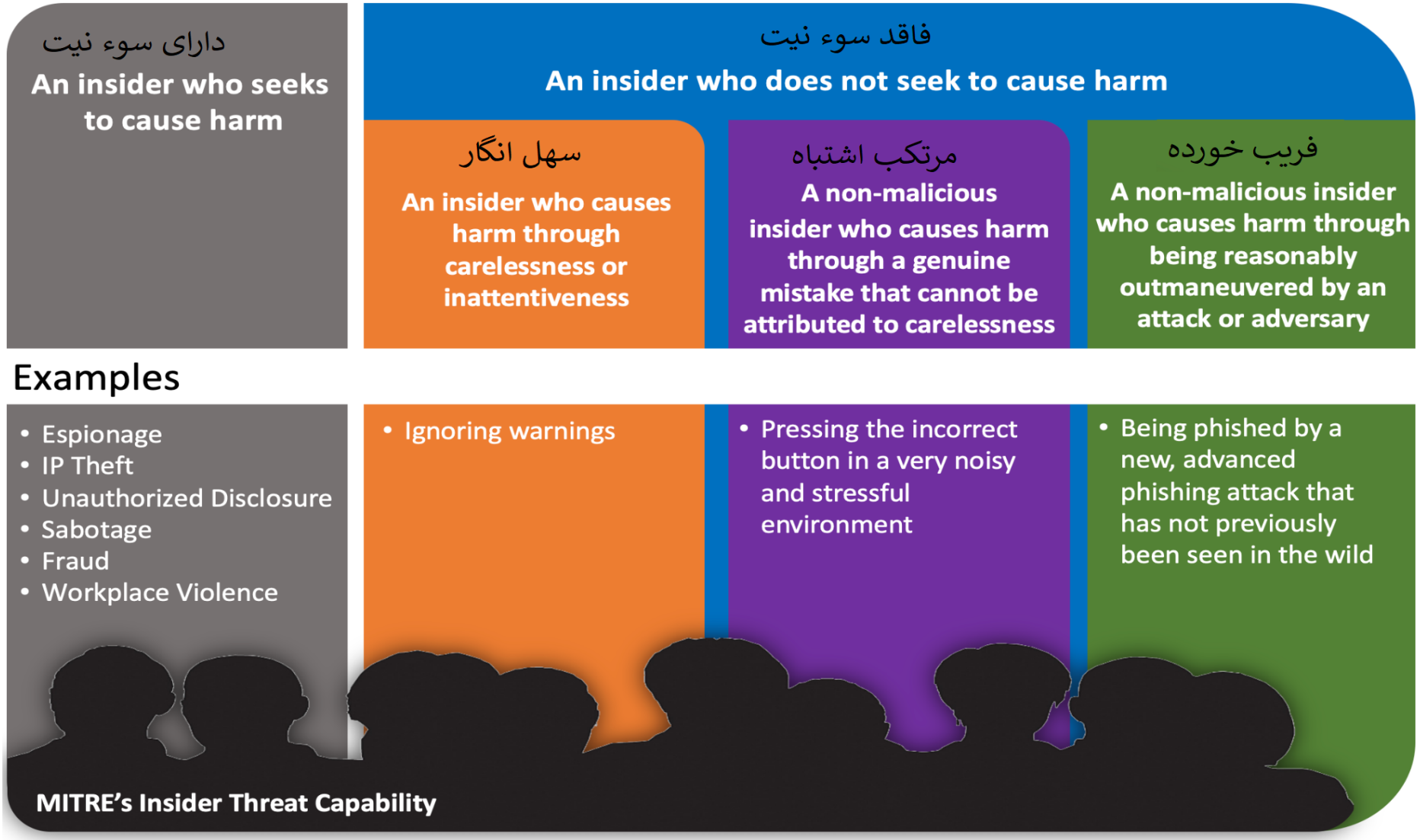
NIST, Cybersecurity Case Studies: Norsk Hydro, NISTIR 8259, 2020

مالی

حمله سایبری به Equifax در 7 سپتامبر 2017، باعث نشت اطلاعات 147 میلیون مشتری و جریمه 700 میلیون دلاری (425 میلیون دلار جریمه، 275 میلیون دلار بازیابی)

NIST, Data Breach Case Studies: Equifax, NISTIR 8204, 2018

دسته بندی Insider Threat از نگاه MITRE



MITRE's Human-Focused Insider Threat Types

4

امنیت سایبری و تحول دیجیتال

مقدمه


How cybersecurity boosts enterprise reinvention to drive business resilience
State of Cybersecurity Resilience 2023

جهان متحول شده است

و امنیت سایبری نیز با آن در حال تغییر است - هرچند، این
تغییر همیشه به اندازه کافی سریع نیست که عملکرد عالی را به ارمغان بیاورد

امنیت سایبری: ضرورت استراتژیک

تضمین موفقیت در تحول

اختلال در بازارکه ناشی از تغییرات فناوری، مقررات پیچیده، تنشهای ژئوپلیتیکی و عدم قطعیت های اقتصادی است، رویکرد سازمانهای جهانی به ریسک و تاب آوری را به بوته آزمایش می‌گذارد.

برای تبدیل شدن به یک cyber transformer چه چیزی لازم است؟

- به‌طور مکرر از خدمات امنیت سایبری به‌عنوان یک خدمت (Cybersecurity-as-a-Service) برای بهبود عملیات استفاده می‌کنند.
- 40٪ از cyber transformer ها از طرف‌های سوم یا ارائه‌دهندگان خدمات مدیریت‌شده برای اداره عملیات امنیت سایبری و رفع کمبودهای نیروی انسانی استفاده می‌کنند، در حالی که این رقم برای سایرین 24٪ است.

امنیت سایبری: ضرورت استراتژیک

قدم بعدی چیست؟

واقعیت این است که اگر به امنیت سایبری به‌صورت جامع نگاه نکنید، نخواهید توانست از کسب‌وکار خود به‌طور کامل محافظت کنید.

5

امنیت سایبری، هزینه یا سرمایه‌گذاری

امنیت سایبری: سرمایه‌گذاری استراتژیک

مزایای مالی

- کاهش 45% هزینه‌های نقض داده با سیستم‌های امنیتی قوی
- کاهش 30% زمان بازیابی پس از حملات

مزایای عملیاتی

- افزایش اعتماد مشتریان: وفادار ماندن 80% مشتریان به سازمان‌های امن
- انطباق با قوانین: جلوگیری از جریمه‌های حاکمیتی و مقررات

Gartner, Critical Capabilities for IT Risk Management, G00758234, 2024

Forrester Research, The Forrester Wave: Cybersecurity Risk Management, Q2 2024

امنیت سایبری، هزینه یا سرمایه‌گذاری

سرمایه‌گذاری در امنیت سایبری (1% بودجه سالانه IT) می‌تواند تا 3 برابر بازگشت سرمایه در سال اول ایجاد کند.

IBM Security, Cost of a Data Breach Report 2024

سیستم ها	هزینه نقض داده
با امن سازی سیستم ها	2.64 میلیون دلار
بدون امن سازی سیستم ها	4.88 میلیون دلار

Forrester Research, The Forrester Wave: Cybersecurity Risk Management, Q2 2024

بازگشت سرمایه(ROI)

صنعت تولید

شرکت Siemens با سرمایه‌گذاری 10 میلیون دلاری در Splunk Enterprise و CIS Controls در 2022، از خسارت 50 میلیون دلاری جلوگیری کرد، که معادل 400% ROI در سال اول است.

Center for Internet Security, CIS Controls v8 Case Studies: Siemens, 2023

صنعت بهداشت

بیمارستان Johns Hopkins با سرمایه‌گذاری میلیون دلاری در Splunk Enterprise و CIS Controls در 2022، از خسارت 30 میلیون دلاری جلوگیری کرد، که معادل 275% ROI در سال اول است.

NIST, Data Breach Case Studies: Capital One, NISTIR 8272, 2022

صنعت مالی

شرکت Capital One پس از نقض داده در 29 جولای 2019، با سرمایه‌گذاری 15 میلیون دلاری در سیستم‌های امنیتی، از خسارات بعدی 100 میلیون دلاری جلوگیری کرد، که معادل 567% ROI در سال اول است.

Center for Internet Security, CIS Controls v8 Case Studies, 2023

6

مهم‌ترین تهدیدات سایبری برای صنایع

توزیع تهدیدات در ایران

تهدیدات	درصد
فیشینگ	70
باج افزار	20
سایر (APT ها، زنجیره تامین)	10

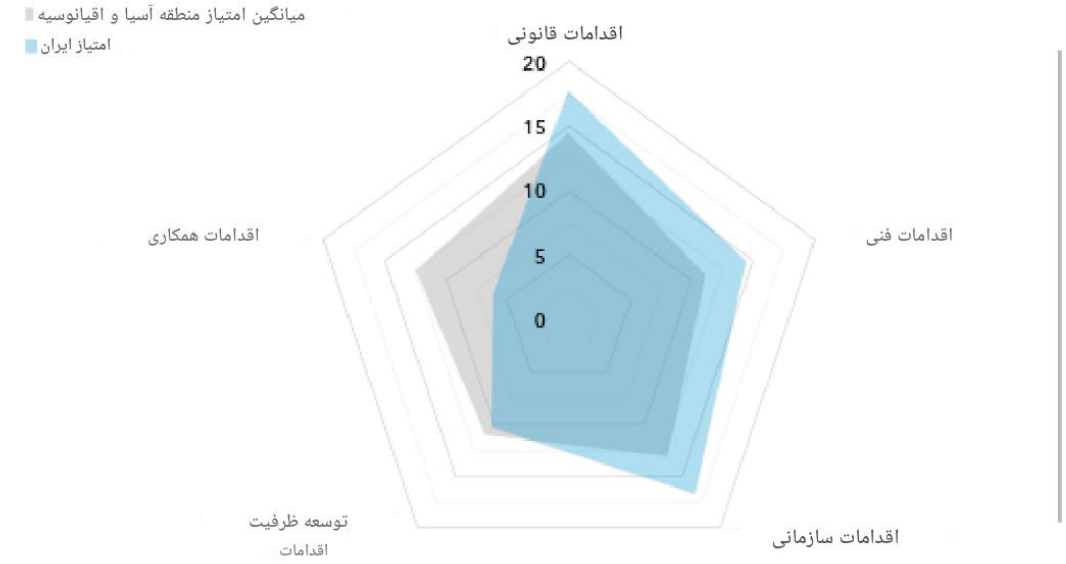
60 % سازمان‌های ایرانی فاقد طرح پاسخ به حوادث.

مرکز ماهر ایران، گزارش سالیانه تهدیدات سایبری، 1403

امنیت سایبری: ضرورت استراتژیک

ایران (جمهوری اسلامی)

پنجمین نسخه نمایه کشورهای GCI



امتیاز کشور

از حداکثر 20 امتیاز برای هر رکن

اقدامات قانونی	اقدامات فنی	اقدامات سازمانی	توسعه ظرفیت	اقدامات همکاری
17.79	14.49	16.72	10.27	6.25

حوزه‌های قدرت نسبی

اقدامات قانونی

اقدامات سازمانی

حوزه‌های رشد بالقوه

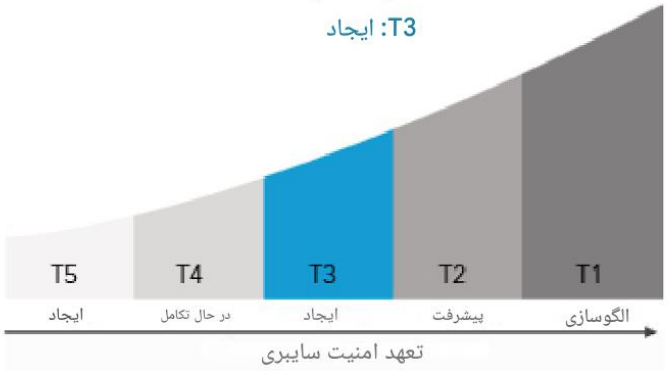
اقدامات فنی

اقدامات توسعه ظرفیت

اقدامات همکاری

سطح عملکرد

T3: ایجاد



*کشورها بر اساس www.itu.int طبقه‌بندی شده‌اند

7

گام‌های عملی ارتقای تاب آوری و امنیت سایبری

گام‌های عملی ارتقای تاب‌آوری و امنیت سایبری

استانداردها و چارچوب ها	توضیحات
ISO/IEC 27001	استاندارد جهانی برای مدیریت امنیت اطلاعات
NIST Cybersecurity Framework	چارچوبی برای شناسایی، محافظت، تشخیص، پاسخ، و بازیابی
ISMS ایران	الزامات محلی برای انطباق با قوانین داخلی

ISO/IEC 27001:2022, Information Security Management Systems, https://www.iso.org/standard/27001
NIST, SP 800-53, Rev 5, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
https://www.ito.gov.ir/fa/isms

گام‌های عملی ارتقای تاب‌آوری و امنیت سایبری

CIS Critical Security Controls

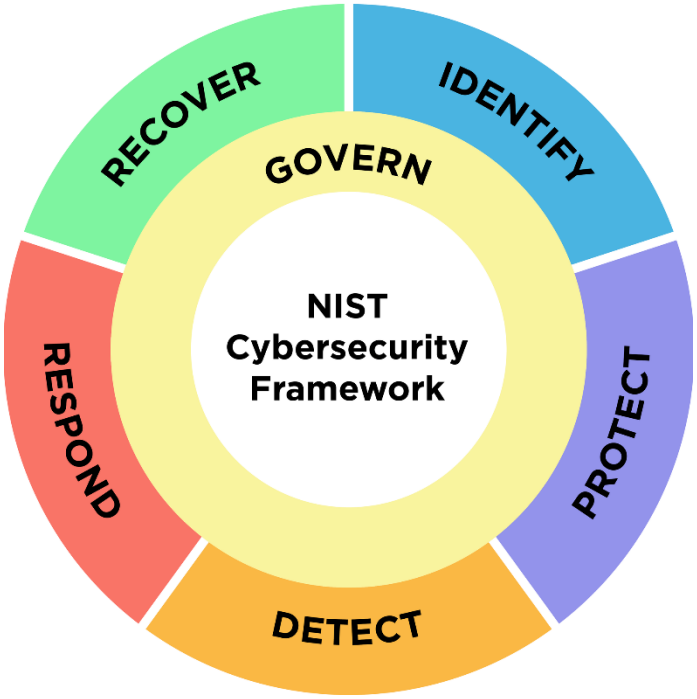
گام‌های عملی ارتقای تاب‌آوری و امنیت سایبری

کنترل های حیاتی امنیت سایبری CIS

پرسشنامه ارزیابی تاب آوری سایبری

https://survey.porsline.ir/s/9HcmbzzF

NIST Cybersecurity Framework

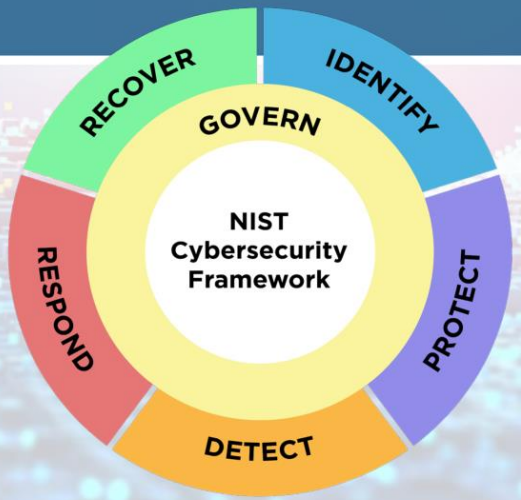


- Govern(حاکمیت)
  - ایجاد و نظارت بر استراتژی مدیریت ریسک
- Identify(شناسایی)
  - شناسایی ریسک‌ها و دارایی‌های کسب‌وکار
- Protect(حفاظت)
  - استفاده از اقدامات حفاظتی علیه ریسک‌ها
- Detect(تشخیص)
  - شناسایی و تحلیل حملات سایبری احتمالی
- Respond(پاسخ)
  - اقدام سریع در برابر حوادث شناسایی‌شده.
- Recover(بازیابی)
  - بازیابی دارایی‌ها پس از وقوع حادثه

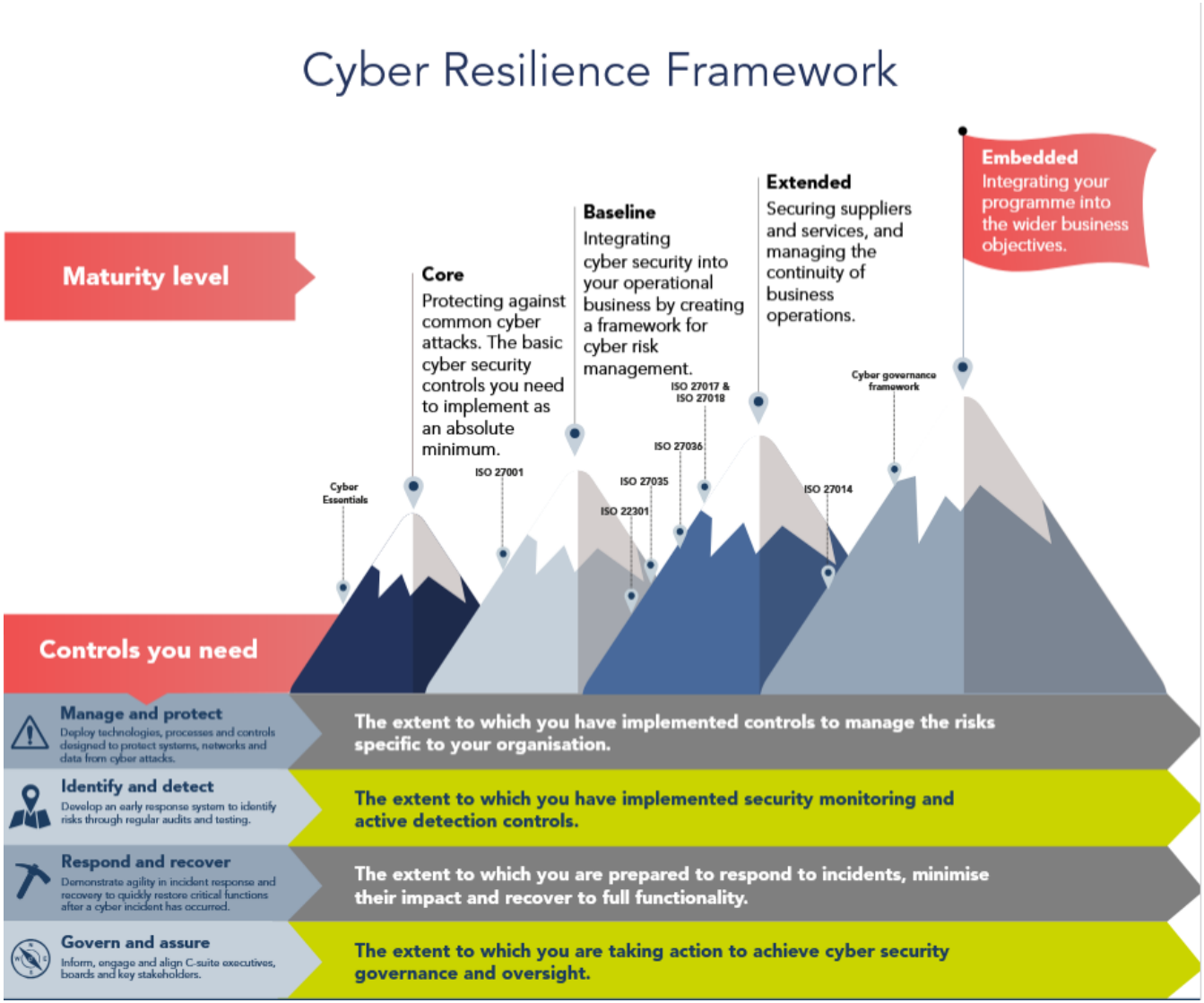
راهکارهای عملی ارتقای تاب آوری سایبری

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide



چارچوب تاب آوری سایبری



چارچوب تاب آوری سایبری

طرح ریزی احتمالی و تاب آوری

- IBM Security. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach
- IBM Security. (2021). X-Force Threat Intelligence Index 2021. https://www.ibm.com/security/data-breach/threat-intelligence-2021
- IBM Security. (2022). X-Force Threat Intelligence Index 2022. https://www.ibm.com/security/data-breach/threat-intelligence
- مرکز ماهر ایران. (1403). گزارش سالیانه تهدیدات سایبری در ایران. https://www.cert.ir/annual-report-1403
- Forrester Research. (2024). The Forrester Wave: Cybersecurity Risk Management, Q2 2024. https://www.forrester.com/report/The-Forrester-Wave-Cybersecurity-Risk-Management-Q2-2024/RES176350
- Gartner. (2024). Critical Capabilities for IT Risk Management, G00758234. https://www.gartner.com/doc/5098234
- NIST. (2018). Cybersecurity Case Studies: Equifax and Maersk, NISTIR 8204. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8204.pdf
- NIST. (2020). Cybersecurity Case Studies: Norsk Hydro, NISTIR 8259. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
- NIST. (2020). SP 800-53, Rev 5: Security and Privacy Controls for Information Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST. (2022). Incident Response Case Studies: JBS Foods, Colonial Pipeline, and UHS, NISTIR 8272. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8272.pdf
- NIST. (2022). Data Breach Case Studies: Capital One, NISTIR 8272. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8272.pdf
- Center for Internet Security. (2023). CIS Controls v8 Case Studies: Siemens and Johns Hopkins. https://www.cisecurity.org/insights/caseitale-studies
- Center for Internet Security. (2024). CIS Controls v8. https://www.cisecurity.org/controls/v8
- سازمان فناوری اطلاعات ایران. (1403). استاندارد مدیریت امنیت اطلاعات (ISMS). https://www.ito.gov.ir/fa/isms
- سازمان فناوری اطلاعات ایران. (1403). گزارش امنیت سایبری صنایع. https://www.ito.gov.ir/fa/cybersecurity-report-1403
- ISO/IEC 27001:2022. Information Security Management Systems. https://www.iso.org/standard/27001
- RSA. (2024). SecurID Suite Documentation. https://www.rsa.com/products/securid
- Splunk. (2024). Enterprise Security Documentation. https://docs.splunk.com/Documentation/ES