The Top Predictions of Cybersecurity for 2024

Oscar Isaka

Gartner®

> **“In order for individuals, institutions, industries, and societies to not only survive but also thrive, it is essential to make peace with uncertainty.”**

— N. Taleb, “Antifragile: Things That Gain From Disorder,” Penguin Random House, 2012

Volatility, Uncertainty, Complexity and Ambiguity (VUCA)

Evolving roles

Emerging technology

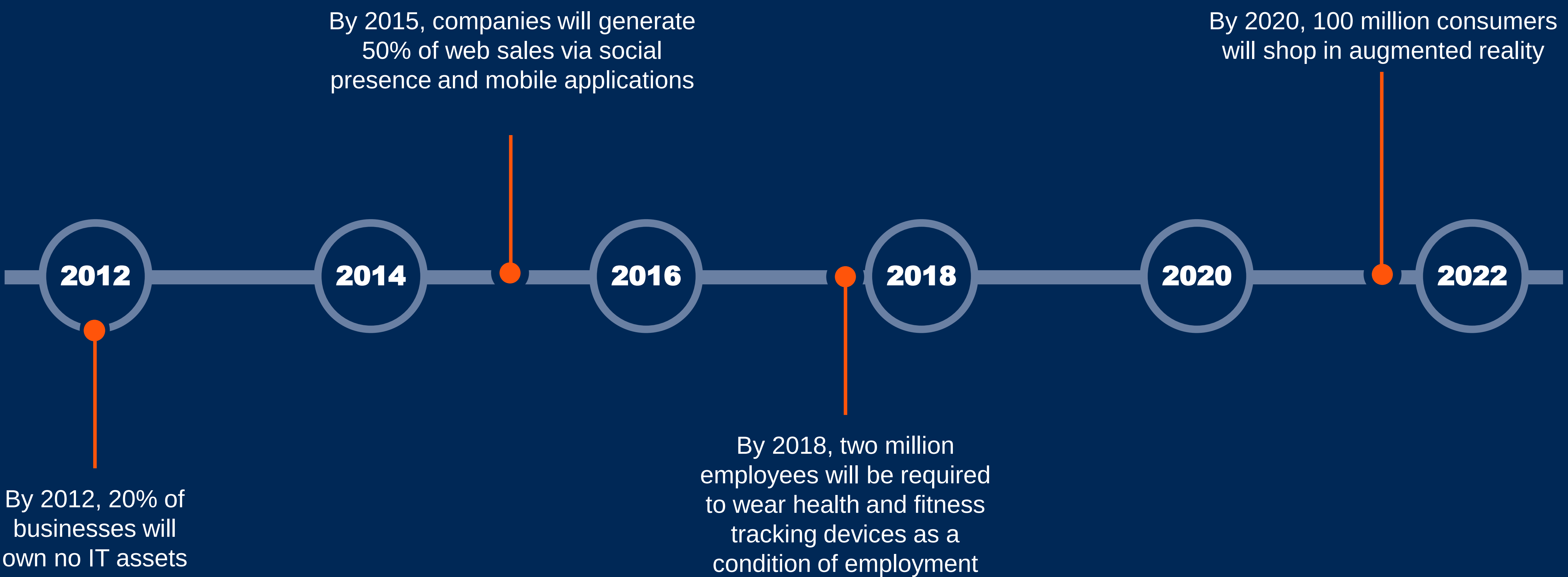
Resilience

Cyber-physical systems

Evolving identity risks

Battling misinformation

Strategic Planning Assumptions — History



By 2012, 20% of businesses will own no IT assets

By 2015, companies will generate 50% of web sales via social presence and mobile applications

By 2018, two million employees will be required to wear health and fitness tracking devices as a condition of employment

By 2020, 100 million consumers will shop in augmented reality

What Does the Future Hold?

Top Predictions of Cybersecurity for 2024+

CISO legal exposure	Battling malinformation	GenAI closes skills gap	Scoping zero trust
2027	2028	2028	2026
GenAI integration	Identity response	DLP and insider risk	Application security
2026	2026	2027	2027

1

By 2027, two-thirds of global 100 organizations will extend D&O insurance to cybersecurity leaders due to personal legal exposure.

Analysis: William Candrick, Alissa Lugo, Lisa Neubauer and Andrew Walls

Legal Disclaimer

Gartner does not provide legal or investment advice.

While Gartner research or guidance may touch upon legal and investment issues, we are not in the business of providing legal or investment advice, and our research or guidance should not be construed or used as a specific guide to action. For all legal issues, we encourage you to consult with your legal counsel before applying the guidance and recommendations contained in our research.

Implications

- Regulators now view cyber risk as a core business risk.
- New laws and regulations expand CISOs’ legal exposure.
- Enterprises must clarify the scope of the CISO role.

Actions

- Redefine the CISO role.
- Consider financial and legal benefits to protect the CISO.
- Clarify roles and responsibilities.

2

By 2028, enterprise spend on battling malinformation will surpass $500 billion, cannibalizing 50% of marketing and cybersecurity budgets.

Analysis: Dave Aron and Leigh McMullen

Implications

- Cybersecurity — social engineering, spear phishing and deep fake fraud.
- Marketing — campaigns and reputation attacks led by corporations or lobbyists impact marketing.
- AI — overwhelming filtering systems through mass production of subversive content.

Actions

- Consistently raising awareness before the board and executive committee.
- Define responsibilities for governing, devising and executing enterprisewide programs.
- Invest in tools and techniques leveraging “chaos engineering.”

3

By 2028, the adoption of GenAI will collapse the skills gap, removing the need for specialized education from 50% of entry-level cybersecurity positions.

Analysis: Nader Henein and William Dupre

Implications

- Advent of GenAI Augments how organizations will hire.
- Mainstream platforms already offer conversational Augments but will evolve.
- This will change how we teach, how we hire and how we specialize.

Actions

- Focus on internal use cases that support users as they work.
- Track homegrown and vendor-provided Augments at the task and role level.
- Coordinate with HR partners.
- Identify adjacent talent.

4

Through 2026, 75% of organizations will exclude unmanaged, legacy and cyber-physical systems from their zero-trust strategies.

Analysis: Katell Thielemann

Implications

- Cloud-based security and dynamic policy enforcements are often undesirable in production or mission-critical environments.
- Not all CPS traffic is IP-based.
- Many older systems have no or limited authentication capabilities.

Actions

- Apply the basics of a zero-trust (ZT) philosophy, but tailor it to non-IT environments.
- Brainstorm with CPS operators and engineers to adapt a ZT strategy to production environments.
- Ask ZT vendors to demonstrate exactly which risks are mitigated for your environment and how.

5

By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs will experience 40% fewer employee-driven cybersecurity incidents.

Analysis: Richard Addiscott

Implications

- Hyperfocused engagement with employees results in improved security behavior and culture program adoption.
- Integration of GenAI capabilities with platform-based architecture can respond to employee behavior.
- Continuously trained LLM supports risk reduction and executive sponsorship.

Actions

- Create a cross-functional working group comprising a suitable cross-section of your organization’s employees.
- Pilot GenAI capabilities augmented by data from multiple sources.
- Leverage GenAI capabilities securely to personalize the communications.

6

Through 2026, 40% of IAM leaders will take over the primary responsibility for detecting and responding to IAM-related breaches.

Analysis: Oscar Isaka and Henrique Teixeira

Implications

- Privilege misuse and stolen credentials remain a top threat.
- IAM leaders often focus on operational metrics.
- CISOs and C-level executives have limited visibility into IAM.

Actions

- Leverage identity threat detection and response practices to build improved capability.
- Provide visibility to the board by leveraging protection -level targets.
- Collaborate with the CISO to align IAM and security initiatives.

7

By 2027, 70% of organizations will combine data loss prevention and insider risk management disciplines with IAM context to identify suspicious behavior more effectively.

Analysis: Andrew Bales

Implications

- Organizations forgo disparate controls, making standalone data loss prevention unappealing.
- Vendors are consolidating user-behavior-focused controls and data loss prevention.
- Combination of controls with context from IAM improves the accuracy of risk mitigation.

Actions

- Identify data and identity risks as the primary driver for data security.
- Evaluate vendors that can address multiple use cases.
- Build multifaceted policies that include layered detection from IAM, IRM and DLP.

8

By 2027, 30% of cybersecurity functions will redesign application security to be consumed directly by noncyber experts and owned by application owners.

Analysis: Christopher Mixter, Deepti Gopal and William Dupre

Implications

- Increased volume equals increased exposure (low code/no code).
- A gap exists between security resources and application teams.
- Increased demand of AppSec professionals.

Actions

- Develop communities of practice.
- Take a minimum effective expertise approach.
- Create a new, high-value role — the “application security product manager.”

Top Cybersecurity Predictions for 2024+

Legal

2/3

of global 100 organizations will extend D&O insurance to cybersecurity leaders.

2027

Malinformation

50%

of marketing and cybersecurity budgets cannibalized to battle malinformation.

2028

GenAI

50%

of specialized education for entry-level cybersecurity positions will not be required.

2028

Zero trust

75%

of organizations will exclude unmanaged and legacy systems from ZT strategy.

2026

Integration

40%

fewer employee-driven cybersecurity incidents from GenAI integration with security behavior.

2026

Identity

40%

of IAM leaders will be responsible for responding to IAM-related breaches.

2026

Insider risk

70%

of organizations will combine DLP and insider-risk disciplines.

2027

AppSec

30%

cybersecurity functions will redesign application security.

2027

> **“The future is already here. It is just unevenly distributed.”**
>
> — William Gibson

Volatility

Uncertainty

Complexity

Ambiguity

A different future awaits …

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Predicts 2024: The Changing Role of the Identity and Access Management Leader**
  Michael Kelley, Rebecca Archambault, Nathan Harris and Others

- **Predicts 2024: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times**
  Deepti Gopal, William Candrick, Andrew Walls and Others

- **Predicts 2024: Zero Trust Journey to Maturity**
  Thomas Lintemuth, Andrew Lerner, John Watts and Katell Thielemann

- **Predicts 2024: AI & Cybersecurity — Turning Disruption Into an Opportunity**
  Jeremy D’Hoinne, Avivah Litan, Nader Henein and Mark Horvath

Access to Gartner research is subject to individual subscription type and product entitlements.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Predicts 2024: IAM and Data Security Combine to Solve Long-Standing Challenges**
  Joerg Fritsch, Andrew Bales, Nathan Harris and Homan Farahmand
- **Predicts 2024: CPS Security — Turbulence Ahead**
  Katell Thielemann, Wam Voster, Ruggero Contu and Wayne Hankins

Access to Gartner research is subject to individual subscription type and product entitlements.