Cyber Security in a changing world

Market trends and strategies

November 2023

Andreas Kronabeter

The world has shifted

and cybersecurity is shifting with it—although, not always fast enough to bring about elite performance.

Market disruption—fueled by technological change, complex regulations, geopolitical tensions and economic uncertainties—is testing global organizations' approach to **risk and resilience**.

Cyber Security is at an inflection point driven by six key market trends

Digital transformation and expanding attack surface

Market Trend 2023

Digital transformation and expanding attack surface

The number of IoT devices worldwide is forecasted to almost triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030.

Statista

What's happening and why does it matter?

- **Complex digital ecosystems** have created **more entry points** and **opportunity for attacks**
- The pandemic has **redefined enterprise boundaries**
- Businesses must **reassess their existing approaches**
- **Organizations are beginning to lack visibility** into activities within their environments
- **Traditional** security **misses a large part of the attack surface**
- An unknown attack surface creates **blind spots** that **hackers can easily exploit**

What can you do?

- **Understand and manage your attack surface** with continuous threat exposure management programs
- **Adopt Zero Trust security** principles to secure the modern digital environment
- **Employ Adaptive Security Operations** to ensure detection of potential blind spots

Shift from technology risk to business risk

Market Trend 2023

Cybersecurity shift from technology to a business risk

88% of boards regard cybersecurity as a business risk rather than solely a technical IT problem.

Gartner

What's happening and why does it matter?

- **Security** is the #1 **business risk** due to shifts in the **geopolitical and regulatory** landscape, and increase in **costs of cybercrime**
- **Increasing number of** sophisticated and complex **threats**
- **Mitigation** requires **company-wide collaboration**
- Cyber incidents cause **serious consequences**
- **Boards** must **manage cyber risks** actively
- Cyber risks are often **not contextualized in business terms,** which prevents the Board from making informed decisions

What can you do?

- Adopt **security risk management program** versus a compliance-driven approach
- **Contextualize cyber risk** in business terms to enable business leaders and the board to make informed decisions
- Promote a **strong cybersecurity culture** to ensure the board, executives, and all employees are actively aware of and trained on the dangers of cyber threats

Responsible adoption of generative AI

Market Trend 2023

Responsible adoption of generative AI to fuel growth & build trust

In just one year, Accenture Cybersecurity Intelligence team saw an **815% surge** in the use of AI technologies **by dark web criminals.**

Accenture Cyber Intelligence analysis 2023

What's happening and why does it matter?

- Adoption of generative AI will **continue to accelerate**, bringing **new frontiers and risks** in the cybersecurity space
- **New opportunities arise,** such as bolstering detection, response and mitigation activities.
- **Without proper data security and regulations,** organizations introduce new risks, including the potential misuse of data
- Organizations must **balance** the **risks and rewards** of generative AI adoption to ensure **ethical and responsible use**

What can you do?

- Ensure **security is "built-in"** to Gen AI projects to enable business agility and scalability
- **Maintain** robust **data security controls** to protect IP and prevent unauthorized access
- **Establish employee training** that outlines the **rules and risks** of using generative AI

Vendor consolidation

Market Trend 2023

Cybersecurity vendor optimization across supply chain

75% of organizations state they are currently pursuing security vendor consolidation; compared to only 29% in 2020

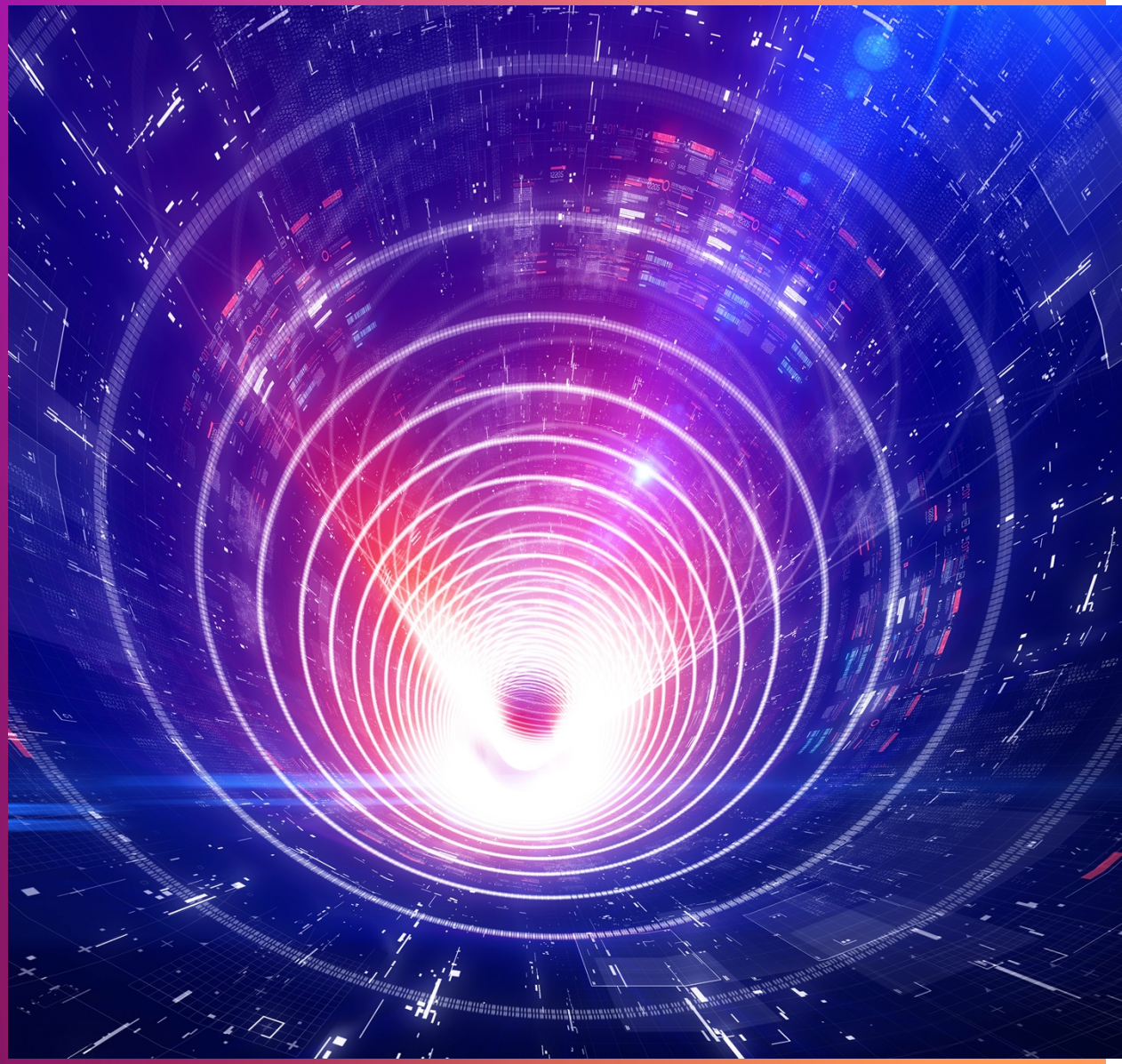
Gartner

What's happening and why does it matter?

- **Focus on consolidation** as **cyber threats** grow and business leaders work with **leaner budgets**
- Organizations seek **simplicity and optimization** in their security stacks
- Many organizations use products from **10 to 20 security vendors**, often with similar or overlapping capabilities
- Challenges include **obscuring the attack surface**, **inadequate integration** of tools, **complex deployments**, **skill gaps,** and **misconfigurations**
- Consolidation **boosts efficiency,** but is a **long process,** with businesses often not seeing the **benefits for several years**

What can you do?

- **Evaluate your security stack** to determine if vendor **optimization/integration is possible**
- Deploy solutions that **integrate disparate security components** into a single, easily managed solution
- Adopt composable architectures, like **Cyber Mesh,** to optimize technology portfolio and enhance the efficiency and effectiveness of security tools



Cyber talent

Market Trend 2023

Cybersecurity workforce retention and enablement

3.4 million global shortage of cybersecurity professionals

ISC² Cybersecurity Workforce Study

What's happening and why does it matter?

- **Recruiting** qualified cybersecurity talent **remains tough,** and **retaining resources** is equally challenging
- Lack of **development opportunities, management support,** and **financial incentives** are top reasons why security professionals leave their jobs
- Cybersecurity is **more than a technology issue; people play a critical role** in the success or failure of **cybersecurity programs**
- High turnover and low employee morale lead to **insider risks** and overall **gaps in cybersecurity coverage**
- People-centric strategies enhance **cybersecurity culture** and **strengthen defenses**

What can you do?

- Transform the **security operating model** by distributing tech and cybersecurity responsibilities across functions
- Focus on **employee experience** to enhance overall company culture and minimize unsafe behaviors
- **Leverage automation** for repeatable processes, allowing cybersecurity teams to focus on tasks requiring deeper level of skills

Global disruption

Market Trend 2023

Global disruption and elevated threat landscape

91% of business & cyber leaders believe that a far-reaching, catastrophic cyber event is somewhat likely in the next 2 years

Global Cybersecurity Outlook Report 2023

What's happening and why does it matter?

- **Global disruption** is at an **all-time high, increasing 200%** in the last **5 years**
- **Geopolitical conflicts** profoundly **affect** cyberspace with battles fought **physically and online**
- Use of **State-sponsored malware** is on the rise
- Heightened uncertainty **increases the risk of severe cyber attacks**
- The impact can be **extreme and far-reaching,** affecting critical industries and costing **millions in damages**
- Public and private sectors must **enhance cyber resilience** to mitigate future disruptions

What can you do?

- **Assess and mitigate risks** associated with third parties and services providers through comprehensive, systemic **third-party risk management approach**
- Maintain strong **cyber** and **operational resilience** with **programmatic detection and response** capabilities

Thank you

Contact Details

Andreas Kronabeter
Senior Manager
Security Lead Austria
andreas.kronabeter@accenture.com
+43676872033840