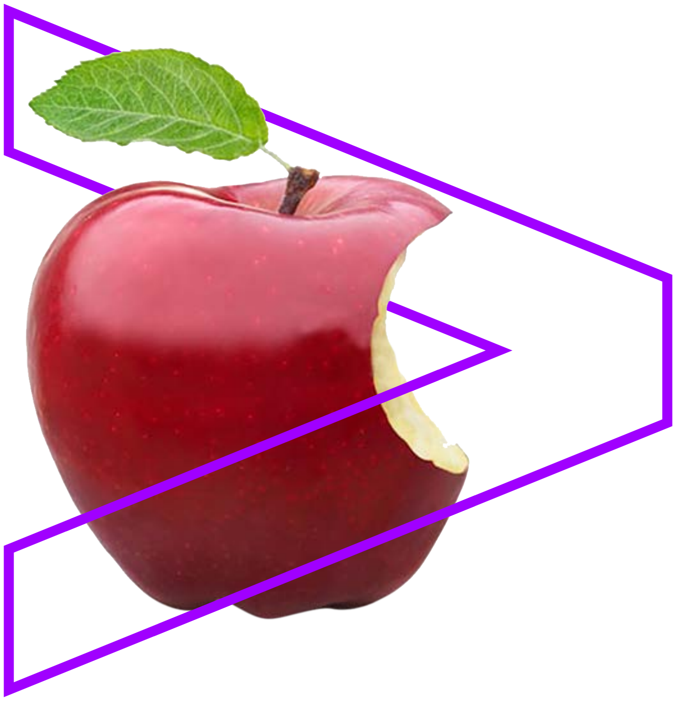
accenture consulting

CONSPICUOUS SECURITY CONSUMPTION

ACHIEVING CYBER RESILIENCE IN CONSUMER GOODS & SERVICES



Infusing security

Decades of mergers, acquisitions, or partnerships have left their mark on the Consumer Goods and Services (CG&S) industry. Many companies find themselves with large, decentralized organizational models that emphasize individual businesses or brands—a modus operandi which has opened the door to increased cyber risk due to inconsistent security maturity across the organization. While security executives are spending time and money on protecting traditional IT services and assets, such as e-mail, IT datacenters, enterprise applications, and desktop environments, many are not addressing new threats that are emerging internally and across the value chain in product development, manufacturing, supply chain, and customer operations—areas which, if breached, could have a material impact on the business.

Business and manufacturing functions are embracing digital technologies—from the adoption of cloud to connected factories and supply chain, to direct-to-consumer channels. And as their organizations transform, so too must their cybersecurity strategies and how they are handled. It is time to elevate the role of the security executive, from IT security leader to a trusted business enabler who can infuse security and cyber risk reduction disciplines into the fabric of the organization's strategy and execution activities. In doing so, CG&S organizations can build a cyber resilient business—one that can operate effectively despite persistent threats and sophisticated attacks, embrace disruption safely, strengthen customer trust and boost shareholder value.

70% **of CG&S executives say that "cyberattacks are a bit of a black box, we do not quite know how or when they will affect our organization."**

84% **of CG&S executives recognize that as companies adopt innovative business models, ecosystems, liquid workforces and so on, the risk and security attack surface area increases exponentially.**

Defending attacks

Organizations are investing in cybersecurity on an unprecedented scale—but current spending priorities show that much of this is misdirected toward security capabilities that fail to deliver the greatest efficiency and effectiveness. A study by the Ponemon Institute and Accenture shows that of nine security technologies identified in a survey, five had a negative value gap where the percentage spending level is higher than the relative value to the business.[1] This issue is compounded by the fact that often security executives do not have either the visibility into the non-IT asset landscape, nor the authority to impact risk outcomes in these areas of the business, despite having a broad risk-reporting responsibility.

Cyberattacks can not only result in operational disruption, but also affect the beating heart of the business. Organizations need to identify and prioritize high-risk areas. They must make sure that they have "a seat at the table" during business planning, strategy and design processes to inform decisions, de-risk innovation challenges, and build a more resilient business. The outcome? A business that is secure, by design.

Areas where a CG&S organization can make a positive impact quickly on its risk posture include:

Secure the journey to cloud

Build trust in direct-to-customer initiatives

Manage operational technology risk

Secure the journey to cloud

Increasing competitive pressures and retail margin compression are forcing manufacturers to examine costs, operations, and capital allocation. The resultant impact can affect the organizational structure, workforce, and the efficiency of their operations. Many C&GS companies see the cost-effective cloud as the answer, moving applications, workloads and, in some cases, whole data centers to third-party providers. As with any major change event, this transition offers an opportunity to reexamine the business—reevaluating its applications, infrastructure, operations, and development practices to put security at the heart—and build the resilient business they want to become.

Rather than simply moving assets "as-is" to the cloud, organizations need to see this as a chance to review risk and prioritize security around their core assets that, if breached or impacted, could result in damage to the organization's financial position, its reputation or industry standing, its legal, contractual or liability status, or the health and safety of its people. And in doing so, they can "design in" the appropriate control structure to mitigate risks, whether preexisting or those that are newly introduced in platforming or simply moving to the cloud.

53% **of CG&S companies identified "better security" as a benefit to be gained from cloud migration.**[2]

Build trust in direct-to-customer initiatives

Many CG&S companies today are creating strategies to deepen direct consumer relationships and to use data analytics to inform the operations of the business. They are bringing this to life with industry initiatives around artificial intelligence (AI), analytics, and machine-learning-enabled initiatives. In this way, they are able to mine large consumer data sets to better engage customers, manage promotions, and understand buying and consumption behaviors. As a result, they are evolving strategies and associated capabilities in support of their digital channels to establish a better, more relevant relationship with end consumers of their products or services—in some cases, without relying on retail partners or distributors.

But while customer data may be the new gold for their marketing campaigns or digital strategies, organizations need to understand and preemptively account for the new risks and protection obligations that come with this or any new data set. Consulting with cybersecurity and privacy teams in the planning and execution of data-driven strategies, rather than introducing them at execution stage, can identify risks and proactively mitigate them early in the innovation process. Prioritizing security-by-design is essential when digital trust and privacy influence consumers' purchasing decisions. Being prepared for new regulations, such as the General Data Protection Regulation (GDPR)[3] or the California Consumer Privacy Act (CCPA)[4], is important, too, as regulators create stringent new rules to protect customers from the theft or abuse of their data.

Above all, the business-minded security executive can help the organization to avoid disruptive or cost-prohibitive remediation activities "after the fact", which is common practice as new regulations are introduced. A security "business partner" can help to inform the strategy, not to interfere with innovation, but to innovate faster. A well-articulated security discipline can also aid in building market trust by advising how the business can enable customers to be informed while protecting themselves.

50% **of security breaches experienced by CG&S organizations have been linked with customer data in the last 12 months.**

Manage operational technology risk

Advancements in Operational Technology (OT) environments have helped CG&S companies to make significant improvements in the quality, uptime and safety of their factories. Now, a new generation of OT is emerging, which includes the introduction of Internet-connected devices and services to enable remote management and monitoring. But with manufacturing's number one priority to keep the factory running, security is rarely top of mind. And as OT networks become less isolated from IT networks, so their vulnerabilities grow. As a result, in recent times security executives have been forced to turn their attention from the IT to the OT environment, which has a unique set of challenges:

A lack of security accountability

Traditionally, many of the activities related to protecting manufacturing centers were not the responsibility of security and were distributed into operations or the business itself, which lacked the resources or skills to support it. Consequently, environments may be ineffectively monitored for threats.

Inconsistent security processes

Governance over security in OT environments is rarely well established, especially in areas such as identity management, change management, and patch management. Industrial change management processes often do not, or cannot, incorporate security. Limited maintenance windows must be carefully managed to prevent operational disruption. Many response plans focus on maintenance, repair and operations but fail to account for cybersecurity events. Devices and applications are not always securely designed.

Inconsistent technical controls

Standard controls in IT security, such as patching, endpoint protection, or network segmentation, are not consistently applied in OT. Many production lines run on systems and platforms that are 10 to 20 years old, where support is restricted or has been discontinued altogether.

Incomplete asset visibility

Visibility into asset inventory and usage can be limited.

The evolving threat environment and associated complexity of attacks is driving up the costs of protecting assets in the effort to build a cyber resilient enterprise. And the nature of cyberattacks is shifting. New malware Petya struck multinationals in June 2017 and had a significant financial impact.

British Manufacturer Reckitt Benckiser estimated US$129,000,000 losses alone.[5] Snack company, Mondelez, reported US$188,000,000 of damages as one of the worm's biggest victims.[6] Other CG&S companies, such as Hamburg-based Beiersdorf AG, also found themselves coping with the fallout of cryptocurrency demands to unlock their systems.[7]

43% **of CG&S executives said that they had suffered interruption of physical operations/shutdown of assets as a result of a breach.**

ONLY 26% **of CG&S executives think they are protecting their physical infrastructures/assets with their cybersecurity strategy.**

Being resilient

It is commonly understood that security is everyone's responsibility, but what does that really mean? In the same way as fiscal discipline, security can—and should—be connected to the very fabric of the business. But weaving cybersecurity into corporate strategy, product design, budgeting and daily business activities may require a cultural mind-set shift, both within the organization and in terms of its associated investments.

Developing a new process around customer engagement? The security executive should help to define and safely release it. Launching a new product or finding a new way to distribute an existing one? The security executive should be involved early on in the vision, design, and development to support secure innovation. Creating new services? Then the security executive needs to be in the room alongside other functional leads to proactively identify and mitigate risks in advance of their development.

Business leaders need to see security executives as trusted business partners—collaborators rather than check mark champions in change management, compliance, or Security Development Life Cycle (SDLC) processes. Security executives must embrace business conversations that clearly identify security risks in a way that is easily digested by the business leaders who are responsible for making those risk and funding-related decisions. A security executive who is articulate in the language of the business, with the business, and for the business can provide clear guidance on cyber priorities and redefine the metrics of cybersecurity success so that it is relevant to non-security stakeholders.

Security must operate from the frontline, not to restrict changes but as the voice of reason on how to make them happen securely. Security can be a business and revenue enabler while, in parallel, driving risks out of the system.

34% **of CG&S executives say that cybersecurity budget authorization is with the CEO/Executive Committee, more than the global average.**

Security first

To achieve cyber resilience, organizations need to embed security and risk management disciplines into all aspects of their business. Security executives need to:

01 Organize

Establish visibility and influence on business outcomes, rather than solely on IT outcomes. Institute mandatory security checkpoints in the development or engineering, procurement and budgeting processes to anticipate or identify new risks before they can arise.

02 Identify

Understand and account for existing assets across the organization and determine risk-based priorities. Do not underestimate the amount of business-critical digital assets that may reside outside of IT's sphere of control and influence.

03 Invest

Become brilliant at the basics by tackling security hygiene and risk management programs. Provide stakeholders with the appropriate tools to understand and mitigate risk and above all, be a consultant to the business—a trusted partner in its success.

04 Institutionalize

Embed security disciplines that address today's needs and have the potential to serve tomorrow's demands. Make security part of the innovation, engineering, business planning, and procurement processes.

For CG&S organizations looking to build a direct channel to the customer and keep the lights on, their security obligations must change—they need to protect high value assets, manage a data-driven landscape and drive a new wave of cyber resilience.

50% of CG&S executives recognize they need to improve on cyber threat analytics and 46% on security monitoring—the "basics" of security programs.

Authors

James Crimens
Managing Director
North America, CG&S Security Lead
james.crimens@accenture.com

Michael Hilkman
Managing Director
CG&S Technology Lead
michael.p.hilkman@accenture.com

Stay Connected

@AccentureConslt
@AccentureCPG

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks. Information regarding third-party products, services and organizations was obtained from publicly available sources, and Accenture cannot confirm the accuracy or reliability of such sources or information. Its inclusion does not imply an endorsement by or of any third party. The views and opinions in this article should not be viewed as professional advice with respect to your business.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at **www.accenture.com**.

Notes

Unless otherwise stated, the statistics in this point of view represent CG&S respondents in the survey report "Gaining ground on the attacker: 2018 State of Cyber Resilience," Accenture.

References

[1] 2017 Cost of Cybercrime Study, Accenture and the Ponemon Institute

[2] Accenture Cloud Readiness survey, 2018

[3] Data protection regulation for Europe which came into effect May 2018

[4] Data protection regulation for the United States due to come into effect January 2020

[5] The untold story of NotPetya the most devastating attack in cyber history, *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] Ibid

[7] WannaCry-Like Cyber Attack Keeps Wreaking Corporate Havoc on Second Day, *Carrier Management*, June 28, 2017. https://www.carriermanagement.com/news/2017/06/28/168568.htm