Electronic Components Industry Association

GIPC

Global Industry
Practices Committee

An ECIA Guidance Document

International Cyber Security Advisory Report

GIPC No. 102 Ed. 1

July 2023

Managing Cyber Security for International Operations

Introduction:
ECIA members, electronic component manufacturers and distributors who have international operations face a broad spectrum of cyber risks that could potentially impact their business operations. These risks can be more complex and challenging due to their international scope. The following advisory report has been prepared as the result of a cooperative effort between electronic component manufacturers and their authorized distributors.

Four Key Areas of Awareness for Executives with International Operations

1. Cyber Threats

Cyber threats in foreign locations become more complex due to differing laws, languages, and customs. Some threats are more prominent than others depending on the country and may require different approaches and strategies to address them adequately. Key areas to be aware of:

a) **Cloud Security**
Foreign laws may require using a local service provider for cloud services. This can add complexity if the cloud service provider has different tools, support models, licensing, etc. Managing new systems could impact the speed of business efforts and potentially create a risk for IT systems if the new environment cannot be secured adequately.

b) **Phishing**
Phishing in a foreign language may leave the cyber team less effective if they cannot read the emails and their tools are unable to translate properly or understand how the attack is being conducted to protect against it. Local languages also need to be accounted for in phishing training to be effective.

c) **Data Localization**
Countries are increasingly requiring foreign businesses to keep their citizens' data in their country. IT systems may not be designed for this scenario. It can also put the company at risk if local data is accessed by foreign parties.

d) **Cyber Fraud**
Some countries do not have strict laws regarding intellectual property or computer crimes. They may target electronic component manufacturers and distributors to access corporate IP, steal data, commit payment fraud, or otherwise obtain components without paying (some of which violate OFAC rules).

e) **Cyber Espionage**
Some governments invest in cyber operations for economic gain, national security, or competitive advantage. Be informed about the threats in the countries you currently or expect to do business in. Unique investments in cyber may need to be made to protect your business.

2. International Laws

Operating in foreign countries necessitates understanding applicable laws and regulations, such as the EU's GDPR, China's Cyber Security Law, China's Data Protection Law (PIPL) or the U.S. California laws (CCPA and CPRA). The engagement of a dedicated internal compliance team or external counsel specializing in international cyber security laws is vital to ensure alignment of your policies and procedures.

Since laws can quickly change, tracking of laws and regular training sessions are crucial to keep your team up to speed with updates and requirements. A robust data management strategy, encapsulating data collection, storage, usage, and transfer with a focus on privacy-by-design and data minimization strategies, is also essential.

Your incident response plan should incorporate steps to manage legal issues, for example notifying regulatory bodies and fulfilling specific disclosure requirements. Privacy Impact Assessments (PIAs) should be conducted to identify potential privacy issues in your operations and formulate risk mitigation strategies.

Lastly, routine external audits can identify gaps in your compliance and help maintain alignment with international cyber security and privacy laws. Keep in mind that this is a complex area and there can be significant penalties for non-compliance, including fines and reputational damage. It's crucial to work closely with legal professionals who specialize in this area to ensure that you're fully compliant.

3. An International Response Plan and Scheduled Tests

In managing cyber threats, the identification and prevention of threats are critical. Equally crucial are swift and accurate detection, response, and recovery from threats.

> *"According to the 2022 Verizon Data Breach Investigation Report (DBIR), the average time to detect a breach has hovered around 85 to 100 days. The DBIR is based on an analysis of more than 79,000 breaches in 88 countries. Approximately 60% of incidents were discovered within days, but 20% could take months or more before organizations realized something was amiss. The human element continues to be a key driver of 82% of breaches, including social attacks, errors, and misuse."*

Upon threat detection, containment measures should be activated to limit spread along with recovery systems and procedures in place, including frequent data backups and the segregation of compromised network areas.

Next is the eradication of the threat by addressing the root cause, and possibly reinstalling system software.

The recovery phase then involves restoring affected systems back into the business environment, monitoring for signs of weakness or compromise, and restoring from clean and known good backups to prevent reinfection.

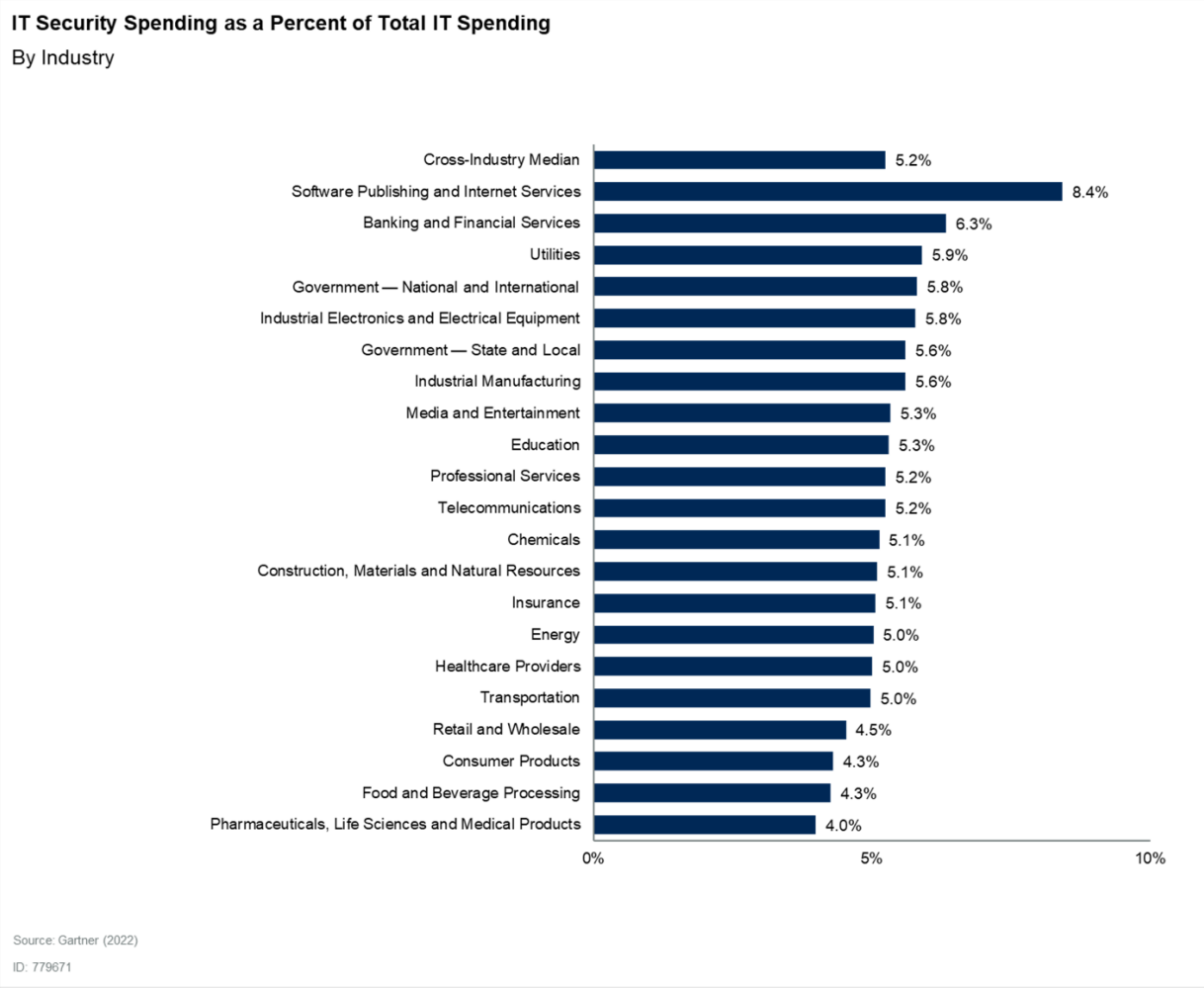
Every incident, regardless of size, should be documented and analyzed to glean lessons for future responses. It is recommended you conduct annual international testing of your response plan, defining clear objectives and including representatives from various organizational sectors internationally. Be aware that time zone differences, languages, varying levels of cyber security maturity, and disparate notification requirements across countries may present challenges that need to be factored into your plan and well-tested.

Additionally, after significant changes in the business (like a merger or a new product launch), it can be beneficial to retest the plan. Smaller tests or drills can be conducted more frequently, such as quarterly. Testing should ideally be done in a way that simulates a real-world attack scenario as closely as possible and involves all the relevant stakeholders (IT, legal, PR, etc.). Following each test, it is essential to review the results, identify any gaps or issues, and update the plan accordingly.

4. Allocating Resources to Protect International Operations

Determining the appropriate level of cyber security investment involves considering multiple factors:

a) Initially, assess industry benchmarks, comparing your cyber security spending to averages for similar-sized organizations in your sector.
b) The cross-industry median for IT security spend as a percentage of total IT spending is 5.2% and 8.4% on the high end for technology companies.
(per Gartner study below)



c) Regular risk assessments will pinpoint areas of heightened vulnerability requiring more resources. Weigh the cost of potential breaches, including indirect costs such as reputational damage and loss of customer trust, against the expense of your cyber security measures to calculate the ROI.
d) Ensuring sufficient investment to comply with regulations in each operating country is essential, as non-compliance can lead to significant penalties. Keep abreast of the ever-evolving threat landscape, investing enough to counter emerging cyber-attacks. Also, evaluate your resource allocation to ensure you focus on the most vulnerable and business-critical areas of your operations. These considerations can guide strategic cyber security investment.

Finally, remember that spending more money on cyber security does not necessarily make you more secure. It is crucial to ensure that the money is spent effectively on measures that genuinely improve your cyber security posture. This might include hiring skilled personnel, investing in advanced security tools, or regular staff training.

A critical part of making your security awareness training most effective is to support local languages for the recipient to ensure higher retention of content. Working with a cyber security consultant can be useful to ensure your resources are allocated effectively.

NOTICE

ECIA Knowledge/Guidance Documents are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for a particular need. Existence of such documents shall not in any respect preclude any member or nonmember of ECIA from manufacturing or selling products not conforming to the documents, nor shall the existence of such documents preclude their voluntary use by those other than ECIA members, whether the document is to be used either domestically or internationally.

This Document is being supplied solely for informational purposes. ECIA assumes no obligation whatsoever to any party or parties adopting or otherwise making use of this Document. ECIA makes no express or implied warranties or representations with respect to the information contained in this Document and expressly disclaims all implied warranties (including, without limitation, any implied warranties of originality, accuracy, timeliness, non-infringement, completeness, merchantability and fitness for a particular purpose). Users of this Document assume the entire risk of any use they may make or permit to be made of the Document or any information contained herein. Without limiting any of the foregoing, and to the maximum extent permitted by law, under no circumstance shall ECIA be liable to any patent owner, or any other person or party, for loss or damage of any kind caused by or resulting from reliance on this Document or any information contained herein.

This Document does not purport to address all issues associated with its subject matter, or use, or all applicable regulatory requirements. No regulatory authority has examined or approved, formally or informally, any of the information set out in this Document. It is the responsibility of the user of this Document to determine the applicability of any regulatory limitations or requirements before its use.

This ECIA Guidance Document was formulated under the cognizance of the Global Industry Practices Committee (GIPC).

Published by:

© 2023 Electronic Components Industry Association
310 Maxwell Road, Suite 200
Alpharetta, GA 30009

Global Industry Practices Committee
The Global Industry Practices Committee (GIPC) provides a forum to discuss processes in the authorized channel that drive best practices within our industry. The GIPC members on this committee work to identify common global problems and issues, formally organize with Subject Matter Experts to research the issues, provide guidance and areas for consideration, and then help drive adoption with the ECIA Board of Directors and Councils. This activity results in the construction of guidelines, specifications, position papers and best practice documents for the electronic components authorized channel. The Committee is made up of executives from four Distributors, four Manufacturers, one Manufacturer's Representative and two ECIA representatives.

Seven Areas of Focus
Technology Solutions – Business Operations – Environmental Compliance – International Trade Compliance – IT Security/Privacy Standards – Logistics Services - Quality

If you are interested in participating in an SME Pool or would like additional information, please contact Don Elario: Email: delario@ecianow.org