Cybersecurity

Risk Management

Communicating Risks

Survey Dates: Aug 1 – Sep 2, 2022

Dale Ford – Chief Analyst

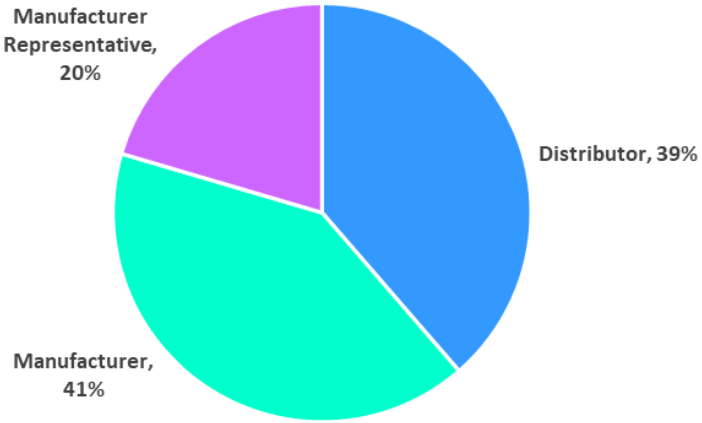
September 7, 2022

ecia

Electronic Components Industry Association

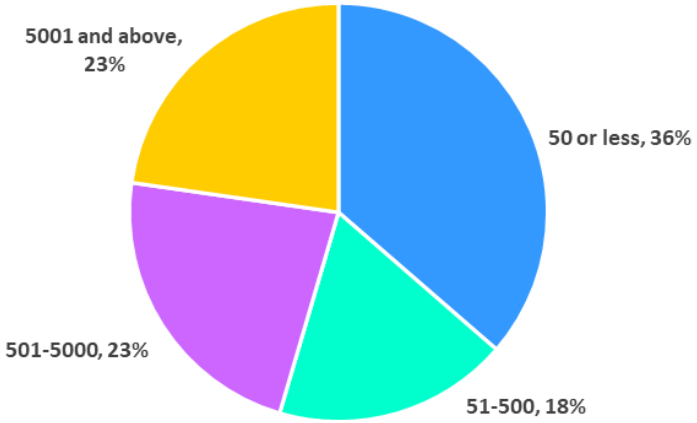
Participant Profile

Participants by Type



TOTAL = 44

All Participants by Size



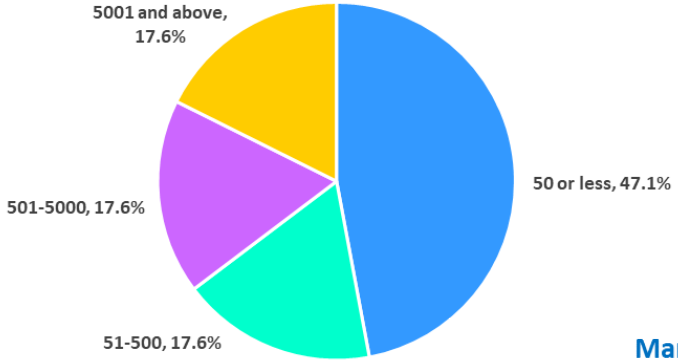
TOTAL = 44

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

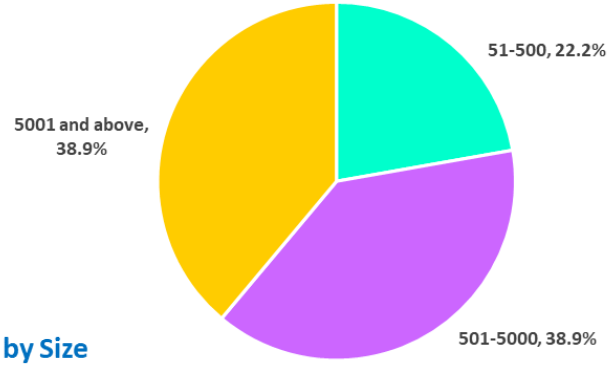
Participant Profile

Distributors by Size



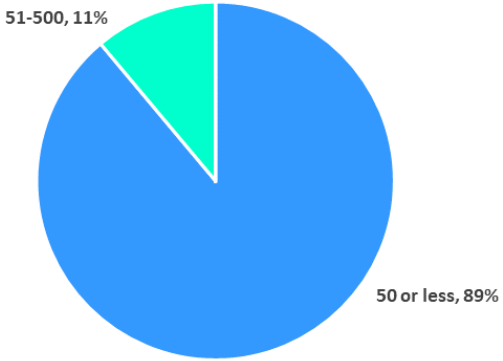
TOTAL = 17

Manufacturers by Size



TOTAL = 18

Manufacturer Representatives by Size

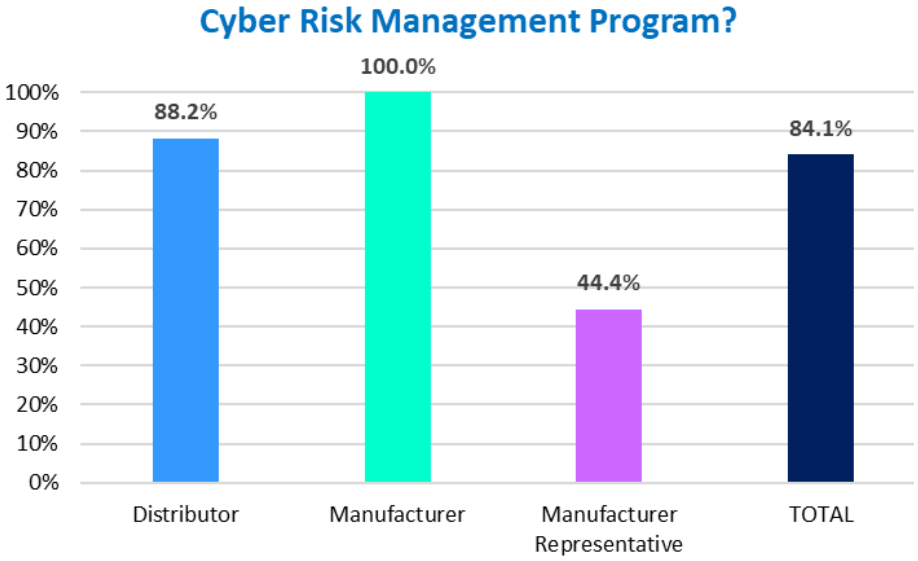


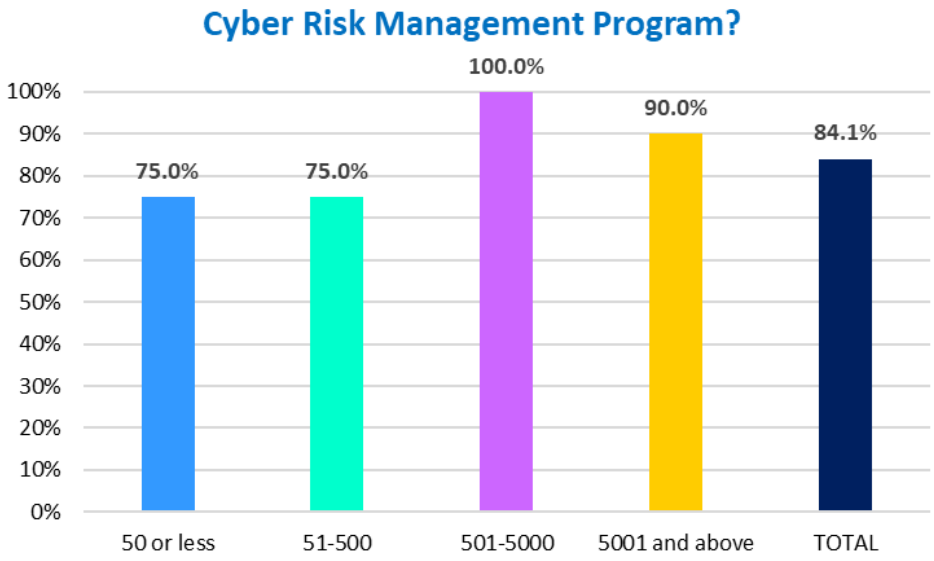
TOTAL = 9

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Companies with a Cyber Risk Management Program





Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Brief Description of Cybersecurity Risk Management Programs

DISTRIBUTORS

- We adhere to the NIST 800 framework and security standards.
- NIST 800-171 and pci-dss 3.2.1 frameworks.
- The program is being developed with a hybrid approach utilizing a few different frameworks (NIST 53, 171, 172 & CSF, ISO, PCI & CMMC, incorporating the most appropriate and best practice controls where they are applicable.
- Cyber Security plan is based on NIST specification, working on CMMC.
- CMMC (NIST-700) compliant. 2 party authentication. process to verify all wire transactions.
- We are compliant to NIST 800-171 and have an SSP and additional policies in place.
- It's based on ISO 27001, PCI and the Top Critical Controls - and is aligned to meet privacy regulations as well.
- Given we interface with Mil Defense contractors and are AS9100 certified, we have a cyber risk plan that involves everything from insurance against attacks, to training of personnel, to software to help us detect bad actors trying to interface with us.
- Documented Risk policy and procedures. Risk Committee meets quarterly. Risk register reviewed and kept up to date.
- Currently working on internal documentation. We also contract with an IT MSP for firewall management and helpdesk services - they conduct annual security reviews.
- We use a 3rd party for training and monitoring our network
- Yes, we do but our IT controls it.

Brief Description of Cybersecurity Risk Management Programs

MANUFACTURERS

- Framework use for cybersecurity program: NIST (US) EBIOS (EMEA & MENA)
- We use the NIST / CIS to 20 framework and controls. We also have a GST (global security team) which operates a SOC out of Japan to monitor logs and global tool deployments. We also have a USST (US security team) which is focused on Norths America activities and policies.
- We tend to follow NIST 800-53/800-171. We also focus heavily on awareness and simulation.
- We use the risk management components of the NIST cyber security framework.
- Our information security and risk program is based on principles from the NIST CSF, ISO 27001, and NIST SP800-171.
- We follow the NIST cyber security risk management framework to guide us through the maturity of cyber program.
- We have a Plan of Action and Milestones (POAM) and System Security Plan (SSP) in place We are working toward CMMC Level 2 certification from the Department of Defense (DoD).
- We have a cyber risk management program based on the ISO 27001 framework. We have implemented an Information security management system that starts with development of an implementation plan. The program involves identification various information security risks and develop risk treatment based upon the risk thresholds.
- We work with a Cyber firm called Solis security that manages the program for VCC.
- In addition to our own IT department, we are working with external partners who manage the global IT framework for RECOM.
- Risk management is run by IT, but with team of sales, operations and accounting personnel.

Brief Description of Cybersecurity Risk Management Programs

MANUFACTURER REPRESENTATIVES

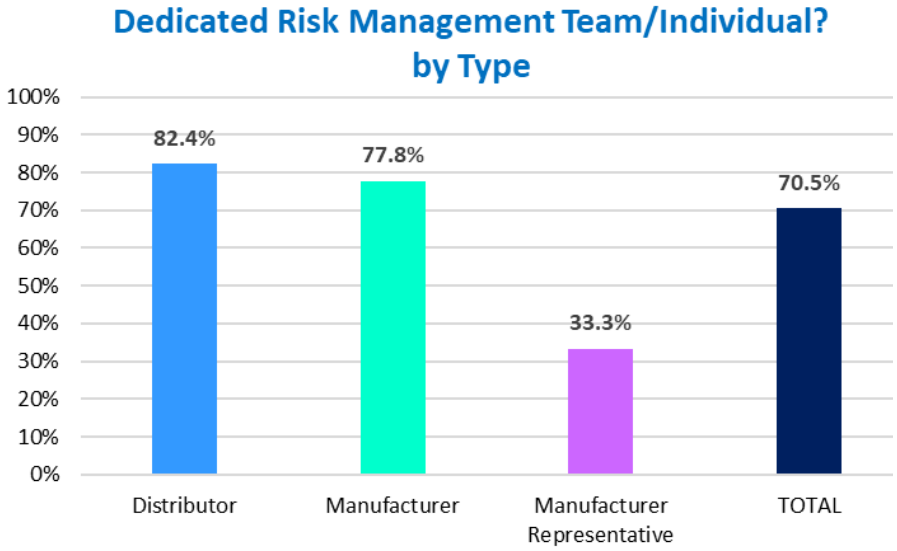
- Partnered with Microsoft Azure Intune for MS products with Azure Active Directory. Partnered with Fortinet with a dual firewall into the building. Full monitoring of all traffic and managed by an outside firm for managed services.
- We are working toward CMMC compliance.
- Our IT team routinely review and discuss current security concerns based on the equipment and technology that we use.
- Outsourced; IT company manages…

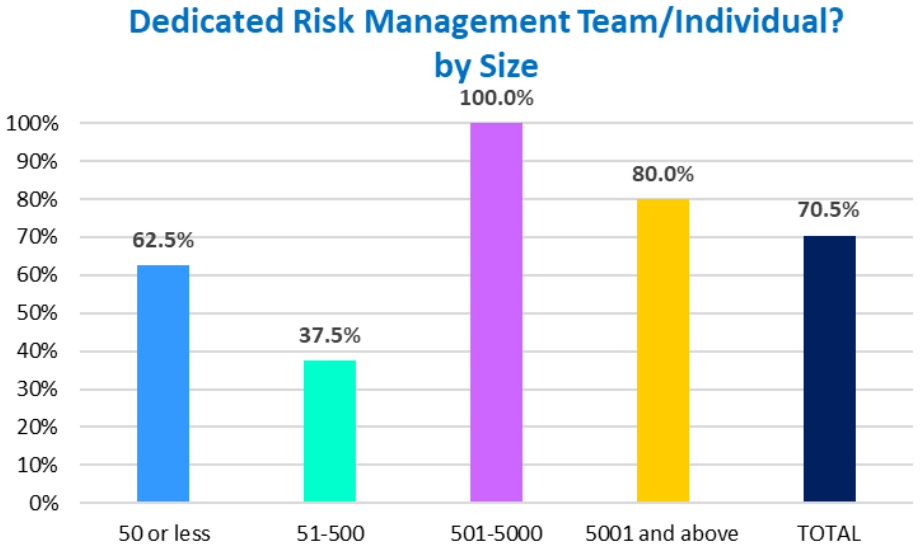
ecia
Electronic Components Industry Association

Interested in Adding a Cybersecurity Risk Management Programs

- According to our IT person (outsourced) - we have pieces that give us a level of protection (MFR REP)
- Yes, it's one of my 'punch items' since taking over. Still in the design phase. (DIST)
- We could benefit from a documented internal program (MFR REP)
- I am interested in what I need (MFR REP)
- It is not on the top of our mind (MFR REP)

Dedicated Risk Management Team/Individual?

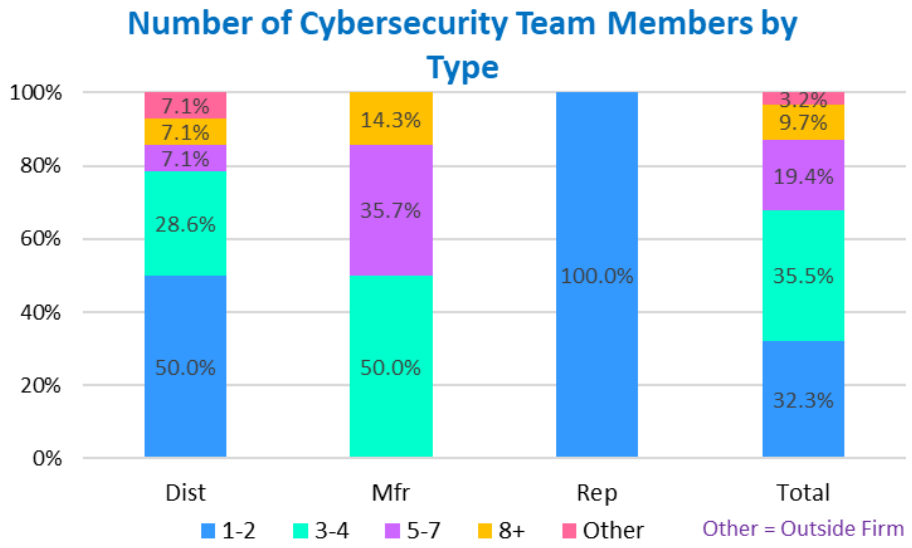


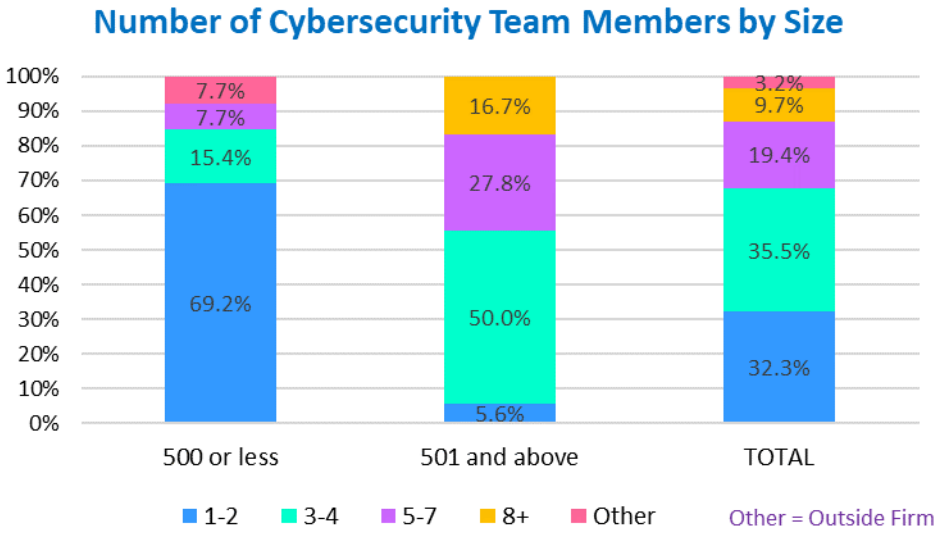


Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Number of Cybersecurity Team Members

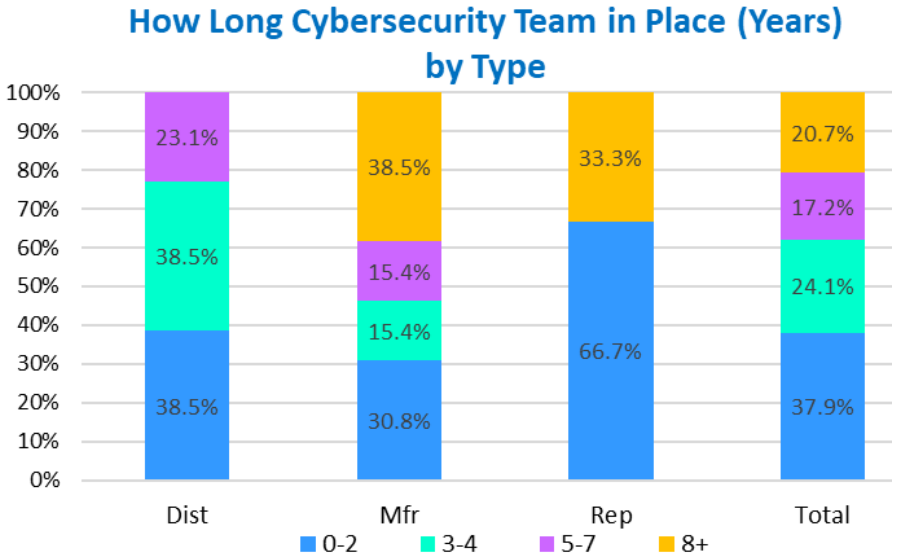


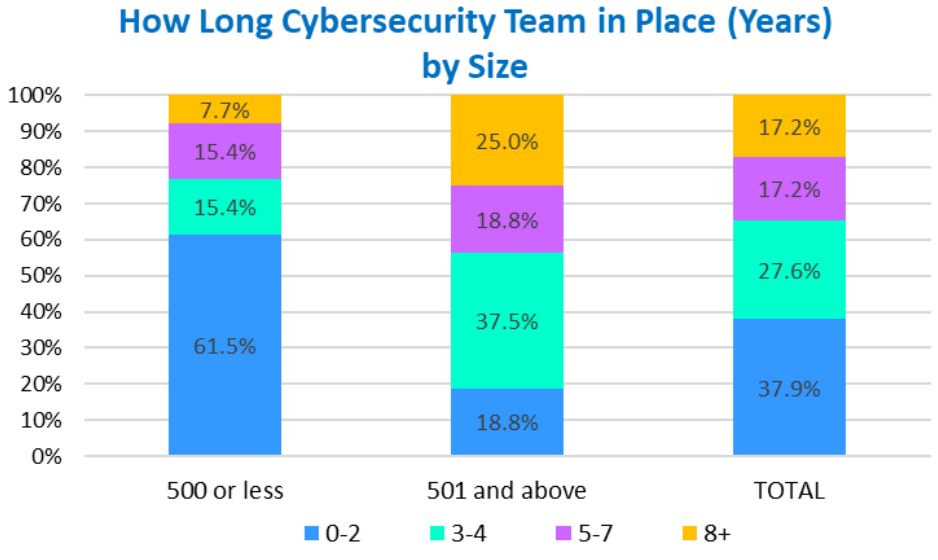


Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Cybersecurity Team Length of Activity





Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

If No Dedicated Team, Who is Responsible for Risk Management?

DISTRIBUTOR

- At this stage it's a mix of IT/Finance/Legal
- A person works with our MSP and manages the cybersecurity. The entire company is trained annually and is aware that they are all responsible for risk management.
- A named individual

MANUFACTURER

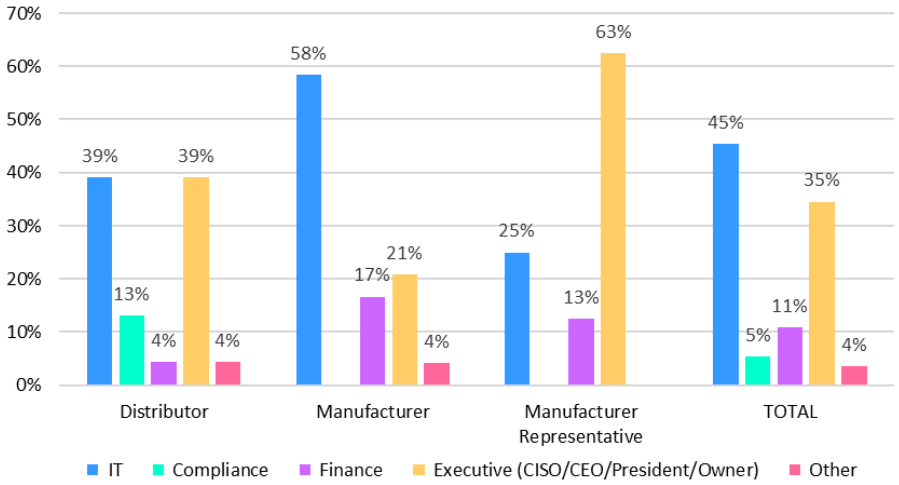
- IT Manager
- External partners do this
- CFO
- Combination of IT Security/Audit/Executive Team

MANUFACTURER REPRESENTATIVE

- Our IT department
- We have one "IT" person that handles all aspects of IT and security
- All of us in the management team, when the matter comes up.
- 3 named individuals

Cybersecurity Team Management Reporting Line

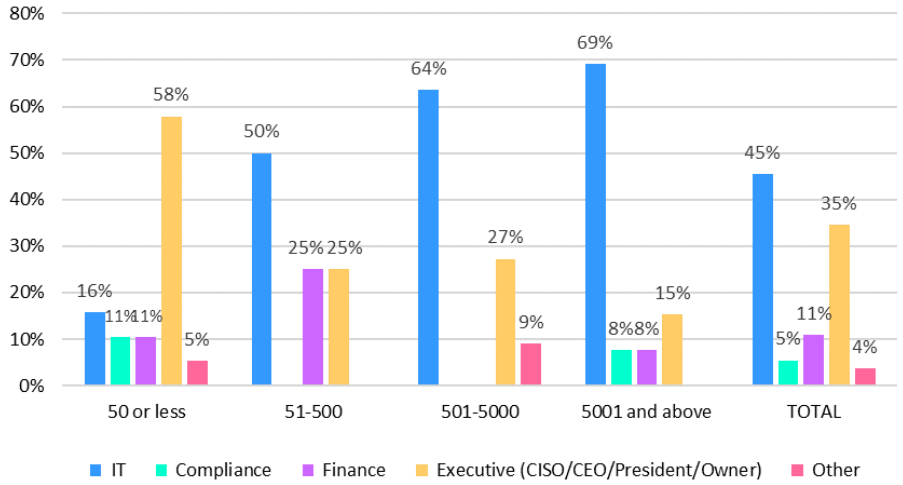
Cybersecurity Group/Individual Reports To - By Type



Note: Sums my be > 100%

Other = Legal; Risk Manager to VP Technical Services to CIO

Cybersecurity Group/Individual Reports To - By Size



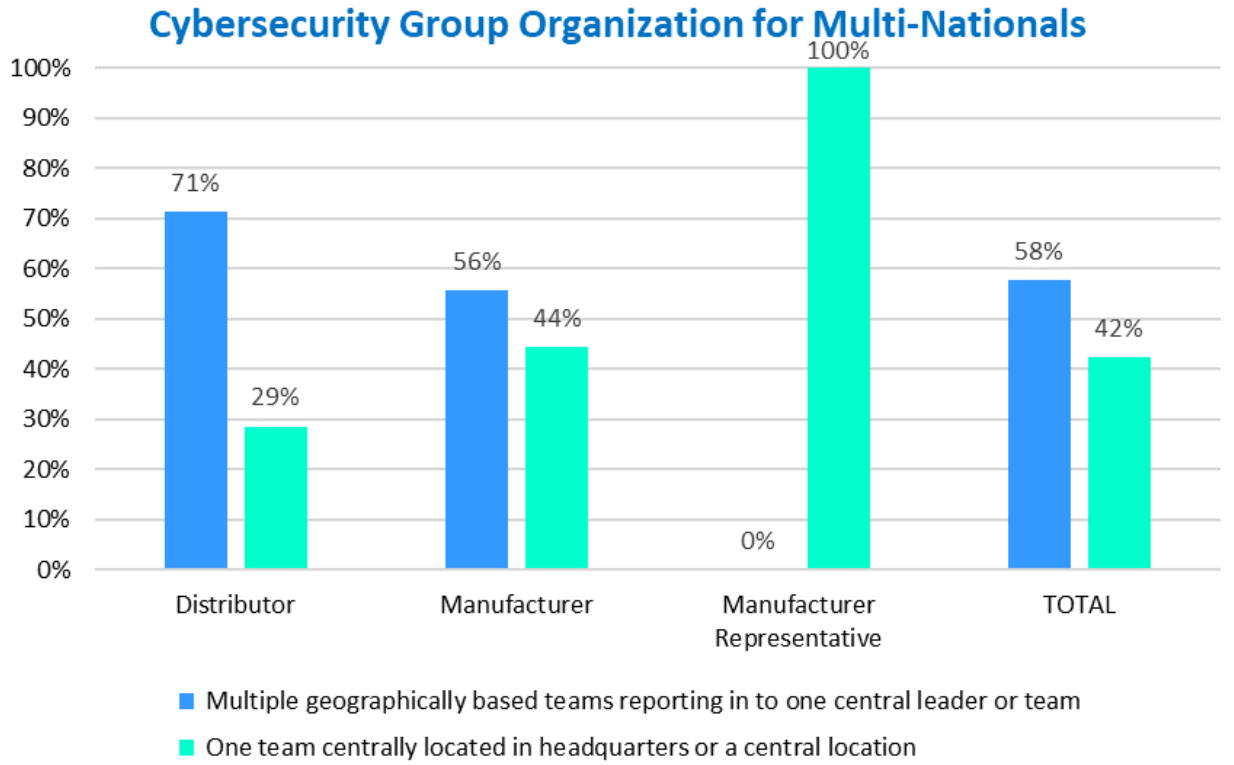
Note: Sums my be > 100%

Other = Legal; Risk Manager to VP Technical Services to CIO

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

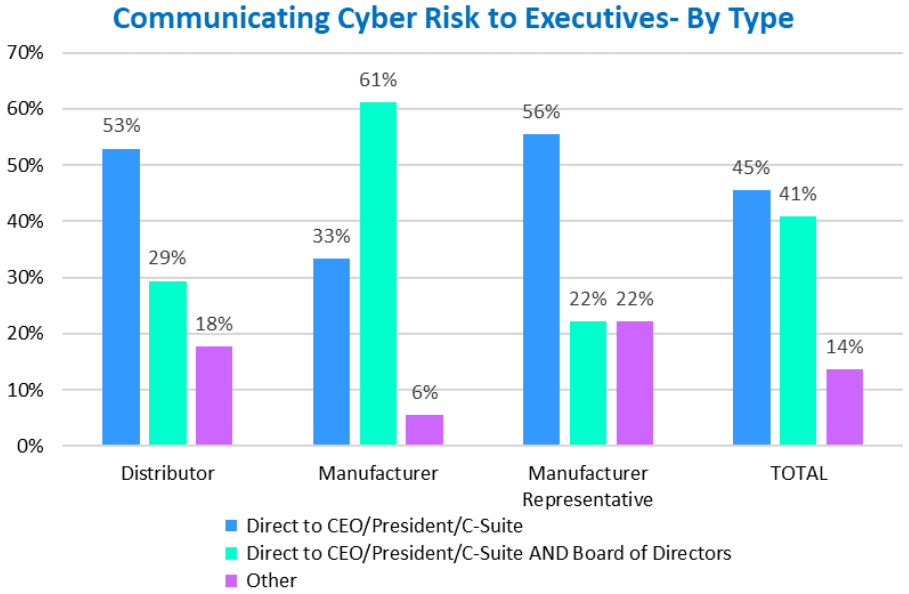
Multi-National Cybersecurity Group Organizations

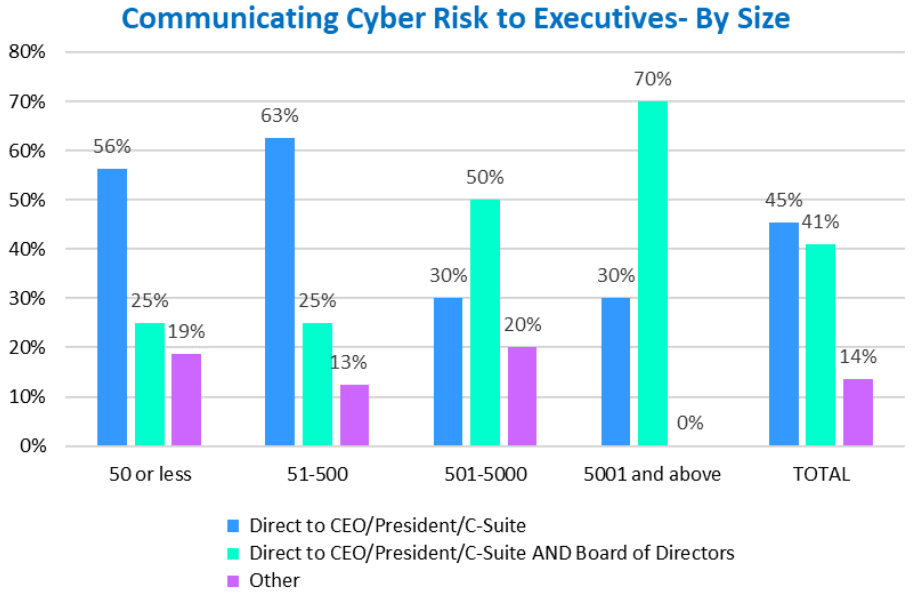


Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Communicating Cyber Risk to Executives



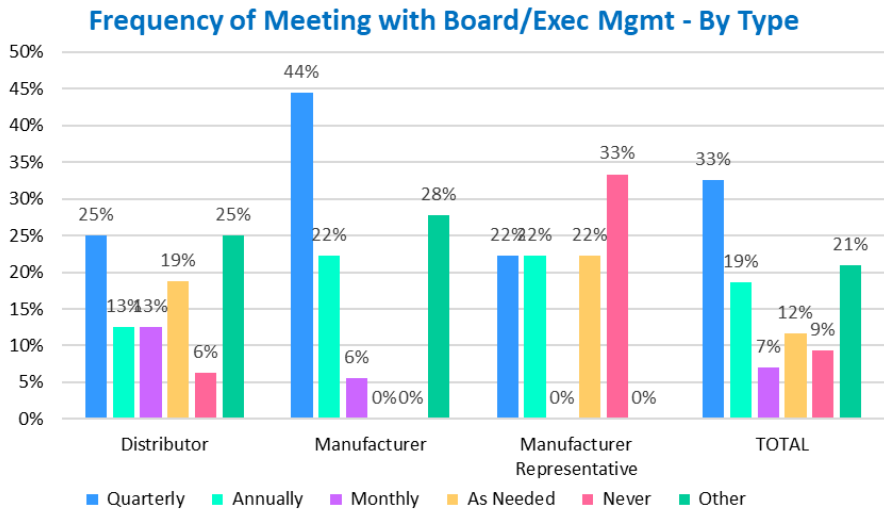


List of Others

- CTO
- Report to the CEO who informs the Board of Directors
- We use our security council as well as our IT Council to communicate security risk and initiatives
- Cyber risks are reported to the leader of IT who reports them to the board and/or direct communications to leadership stakeholders.
- We are a small firm.

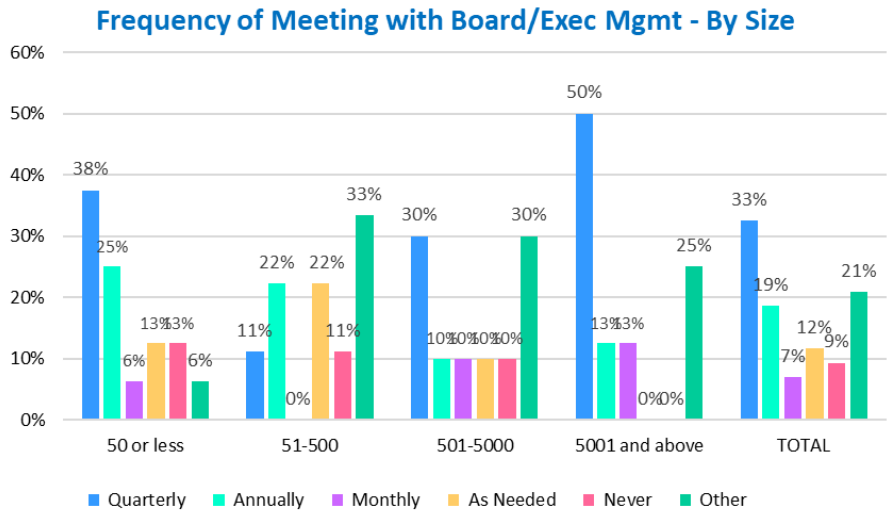
ecia
Electronic Components Industry Association

Frequency of Meetings with Board / Exec Mgmt



Note: Sums my be > 100%

Other = Legal; Risk Manager to VP Technical Services to CIC



Note: Sums my be > 100%

Other = Legal; Risk Manager to VP Technical Services to CIO

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

List of “Others” for Frequency of Board / Exec Mgmt Meetings

DISTRIBUTORS

- We are a family business....every lunch
- Cybersecurity risks are communicated to the executive leader team weekly.
- IT Council meets twice a month and the security council meets twice per year.
- It was quarterly prior to Covid. We are rethinking our reporting and governance and will resume once we have a new approach solidified.

MANUFACTURERS

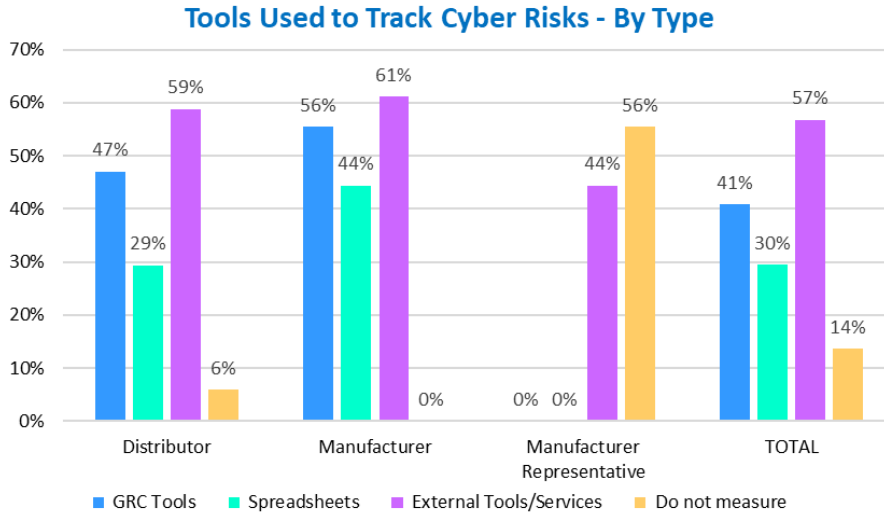
- Often!
- Frequently
- MEA conducts monthly management (MMM) meetings and quarterly executive meets (QMM). Communication on security and other topics are conveyed in these meetings. IT also has a monthly meeting with Presidents\CEO.
- 2-3 times a year
- Semi-annually

MANUFACTURER REPRESENTATIVES

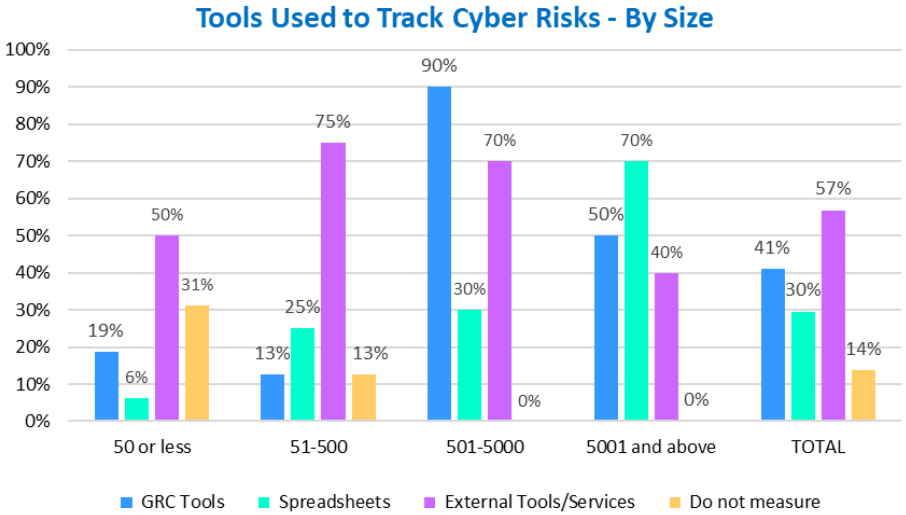
- Only when something would happen, it would be discussed.

ecia
Electronic Components Industry Association

Tools Used to Track Cyber Risk



Note: Sums my be > 100%

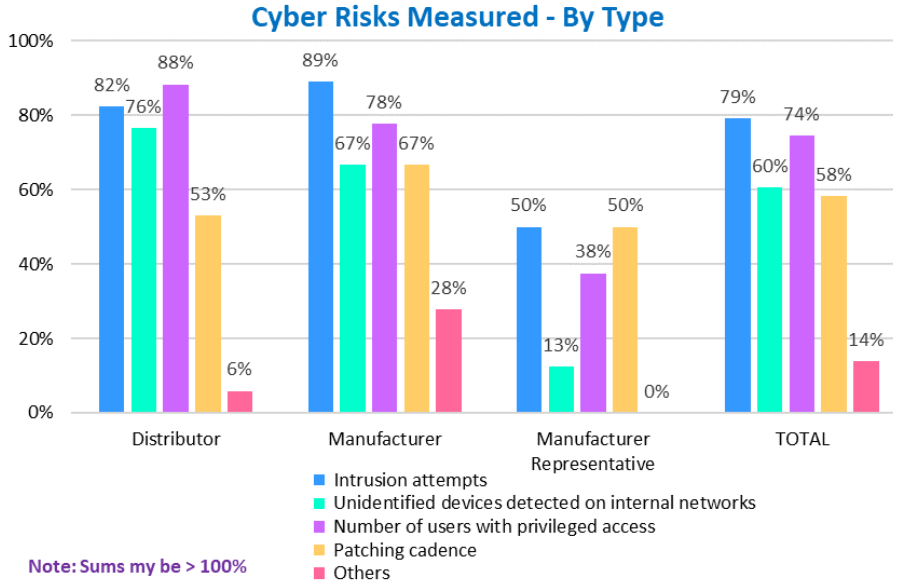


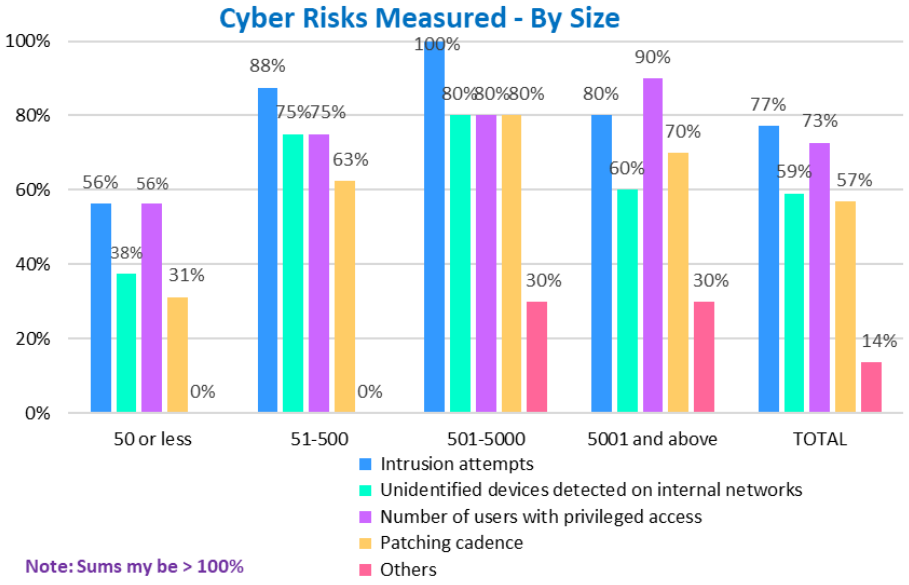
Note: Sums my be > 100%

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Cyber Risk Measurements





Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

List of “Other” Cyber Risk Measures

DISTRIBUTORS

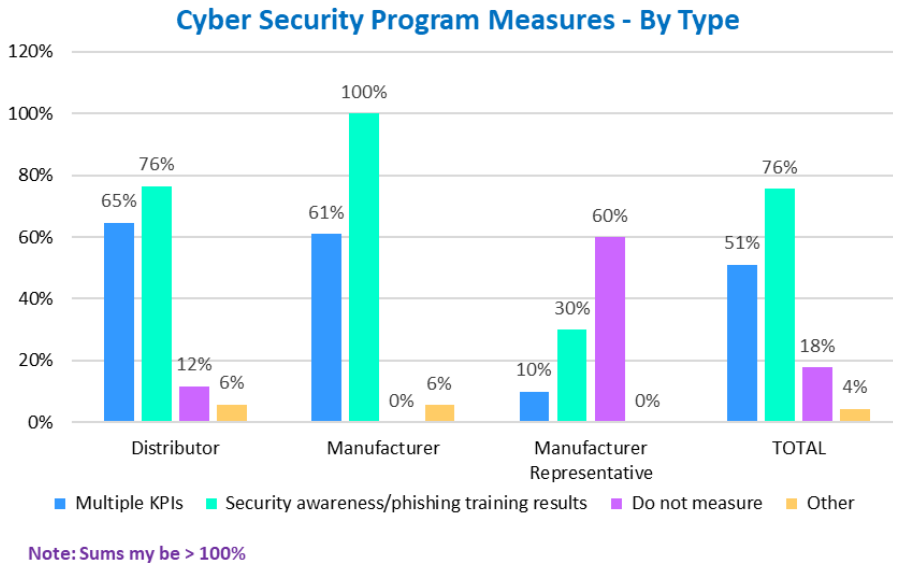
- There are approximately 100 metrics we track.

MANUFACTURERS

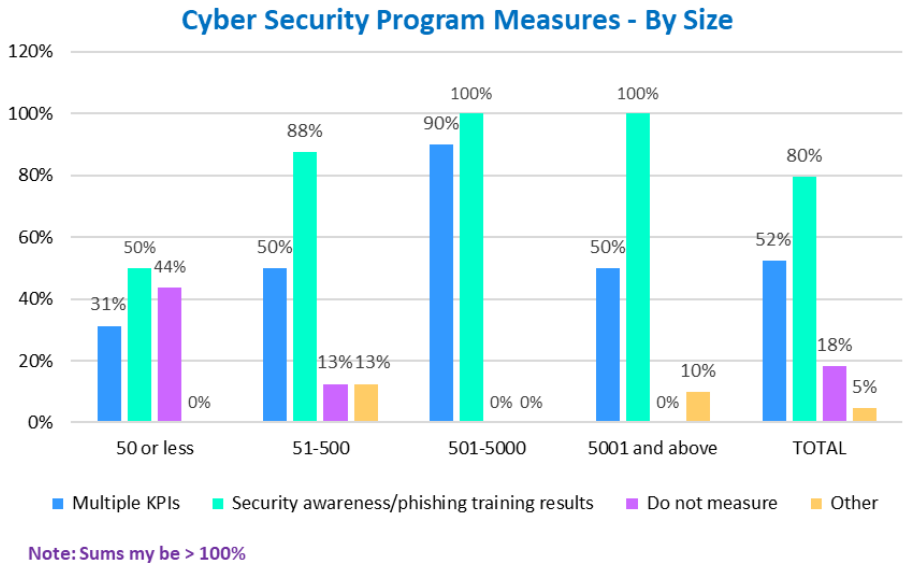
- Vulnerabilities resolved/mitigated (CVEs) - Phishing/Malware emails blocked - Cloud firewall threats - Fraudulent business domains - Best security practice implementations - Data Loss Prevention
- Phishing attempts Threat & Vulnerabilities
- We are deploying the CIS top 20 control framework. With this we monitor several area and are continuing to add more.: -Backup completion and testing -Vulnerability scanning and remediation -security tool operation and installation -Installed SW (approved list) -ITM (User behavior and exfiltration)
- #'s of unresolved patches; Incident Rates; Systems w/Unresolved Threats (XDR); Sandboxing Statistics (Critical/High/Medium/Low); Honeypotting Statistics (Dependent on Network Type); SSL/TLS Certificate Issues; Data Volumes; Inactive User Accounts; Login Failures
- Number of vulnerabilities; Number of zero-day threats encountered; Number of security incidents

ecia
Electronic Components Industry Association

Cyber Security Program Measures



Note: Sums my be > 100%



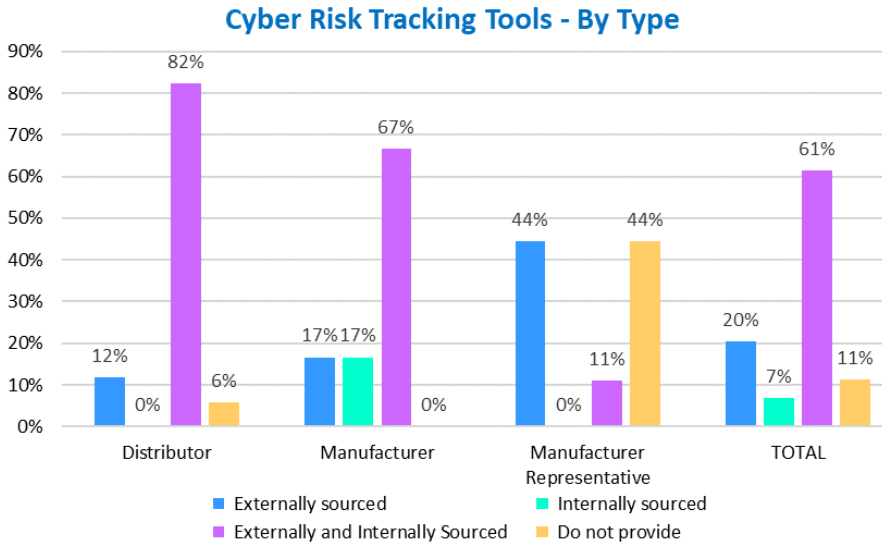
Note: Sums my be > 100%

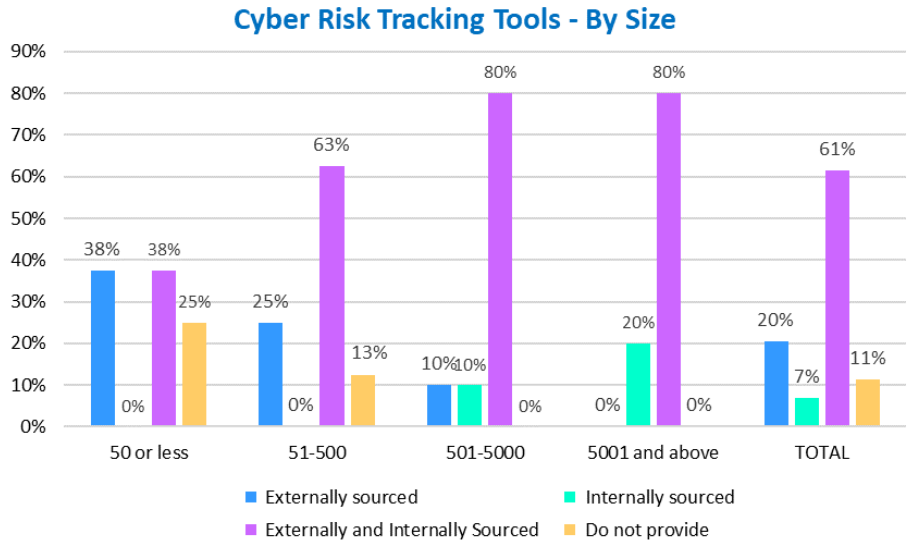
Others

- At this time, it is unmeasured, but it will be with development of the program.
- Monthly mandatory training
- Number of vulnerabilities; Number of zero-day threats encountered; Number of security incidents

ecia
Electronic Components Industry Association

Cyber Risk Tracking Tools

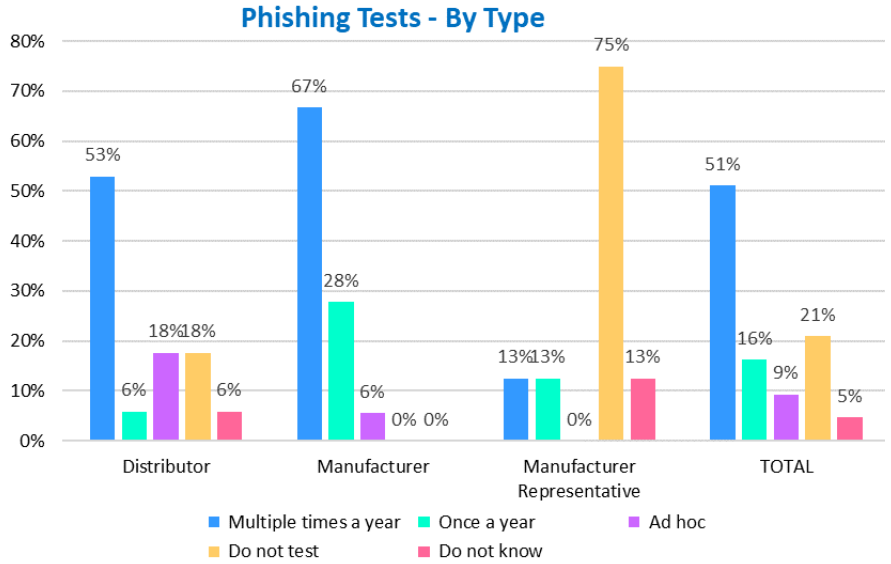


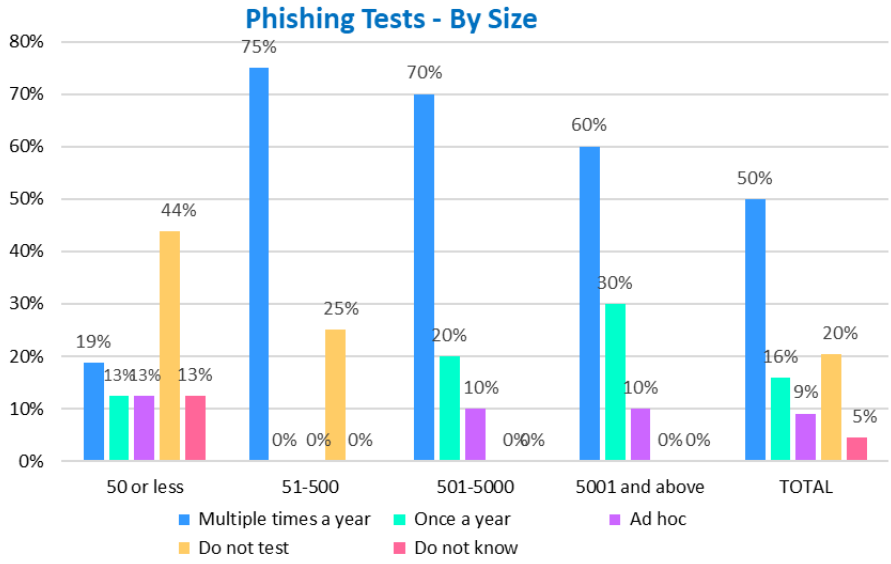


Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Phishing Test Frequency

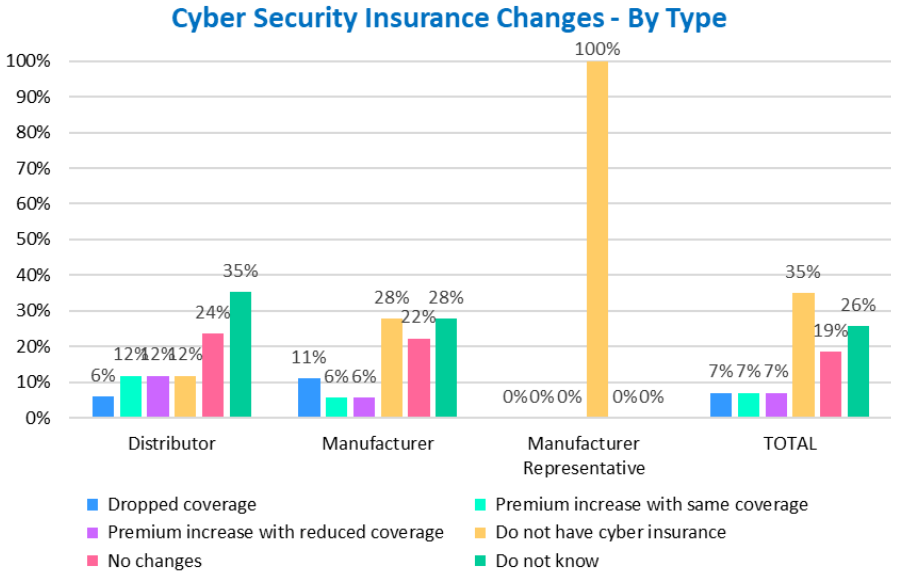


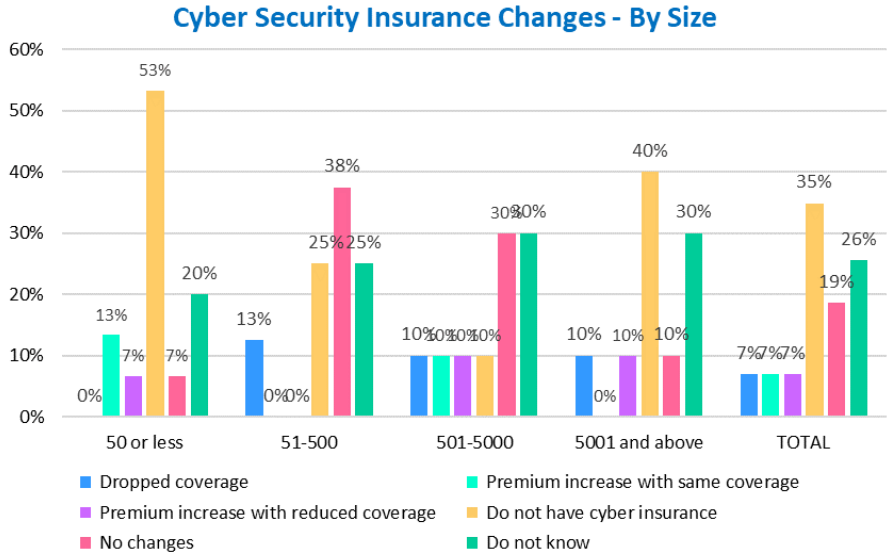


Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association

Cyber Security Insurance Changes





Added Notes

We added cybersecurity insurance to our plan.
We did not find the value of insurance.

Global Industry Practices Committee (GIPC)

ecia
Electronic Components Industry Association