EXECUTIVE SUMMARY
Survey #1 Communicating Risks

- Participants by Type:
  - Manufacturer 41%,
  - Distributor 39%,
  - M-Rep 20%
- Companies with Cyber Risk Management Programs:
  - Manufacturer 100%,
  - Distributor 88%,
  - M-Rep 44%
- Majority of companies are using information and/or guidance from:
  - **NIST CSF 800-171** (National Institute of Standards and Technology Cybersecurity Framework)
  - **ISO/IEC 27001** (IT Security, Cybersecurity and Privacy Protection)
  - **ENISA** (European Union Agency for Cybersecurity)
  - **CMMC** (Cybersecurity Maturity Model Certification) for Department of Defense (DoD) Contractors, Subcontractors and Vendors
- Companies with a Risk Management team and/or individual:
  - Manufacturer 78%,
  - Distributor 82%,
  - M-Rep 33%
- Companies with a Risk Management team and/or individual by size:
  - 5,001 and above 80%
  - 501 to 5,000 100%
  - 51 to 500 38%
  - 50 or less 63%
- **65%** of Risk Management teams have been in place for approximately **0-4 years**.
  - **58%** of Risk Management teams for Manufacturer report into IT while **21%** report into CISO/CEO/President.
  - **39%** of Risk Management teams for Distributor report into IT while **39%** report into CISO/CEO/President.

- Majority of companies communicate risk management direct to CEO/President/C-Suite and Board of Directors.
- Frequency of meetings with CEO/President/C-suite and Board of Directors ranges from monthly-to-quarterly-to-annually-to-as needed; quarterly seems to be most used today.
- **Tools used to track cyber risk is an area of opportunity and further development is needed.**
- Top 4 cyber risk measurements:
  - Intrusion Attempts
  - Unidentified devices detected on internal networks
  - Number of users with privileges access
  - Patching cadence
  - There are over a 100 measurements tracked
- **Cyber risk metrics are becoming more common and widely adopted by organizations.** There appears to be an opportunity for industry standards which can be used for benchmarking, trends, and early warning in the industry.
- Majority of companies run phishing tests multiple times during the year.
- Cybersecurity insurance seems to be a moving target in today's security landscape. From premiums increasing for the same coverage and/or reduced coverage to companies investigating self-insuring to dropping their insurance coverage.
- **With larger companies having more mature cyber risk management programs than smaller companies, there is an opportunity for this work group to provide a base line of cybersecurity practices.**

GIPC Cybersecurity Work Group

Our Core Team

Brad Waisanen, VP, Global Cyber Security, TTI Inc. **(Leader)**
Peter N. Tiller Jr., GM, Business Engineering & Information Technology, Murata Electronics Americas
Bert Kraemer, Senior Vice President IT and CIO, Vishay Intertechnology
Jeff Johnson, Director, IT Security & Privacy, Digi-Key Inc.
Andrew Hester, Director, Networking & IT Security, Mouser Electronics, Inc.
Randall Smith, System Administrator, Luscombe Engineering
Rich Smith, Cybersecurity Manager, Panduit
Rich Breske, Network/Systems Manager, Marsh Electronics, Inc.
Sean Smith, Global Security Team, Murata Manufacturing, Co.
Gautam Vora, Management Information Systems, TDK USA Corp
Jose Romero, IT Operations and Security, Crouzet
Kenneth Kong, Sales Operations Manager, TTL Teck-Tek LTD

ecia
Electronic Components Industry Association

EXECUTIVE SUMMARY
Survey #2 Ransomware Readiness

- Participants by Type:
  - Manufacturer 39%,
  - Distributor 39%,
  - M-Rep 23%
- Participants by Size:
  - 45% less than 50 employees
  - 18 % more than 5,000 employees
  - the rest equally spread by 18%
- 88% of companies with 5,000+ employees perform table-top exercises annually which is a discussion-based session of roles and responsibilities during an emergency.
- 75% of companies with 50 or less currently do not perform table-top exercises and 20% do something other than.
- Majority of companies conduct table-top exercises for a half day.
- For ransomware attacks, how would your company respond to payment demands;
  - 63% of Manufacturers said they would never pay 31% said It would depend on the circumstances;
  - 53% of Distributors said they would never pay 24% said it would depend on the circumstances
  - 44% of M-Reps said they would never pay 22% said it would depend on the circumstances
- On average **63%** of companies surveyed **have not** experienced a ransomware attack; while **20%** **have** experienced a small scale/isolated incident; trends indicate ransomware attacks will increase.
- **38%** of companies 51-500 employees **have** experienced large scale incidents.
- Manufacturers and Distributors have larger incidents, but their attack surface is significantly larger. **Just because you are smaller, does not mean you are not at risk.**

- **Industry average by size and type says it will not pay ransomware demand**…Is this core principle or significant confidence in systems/procedures?
- 100% of Manufacturers and Distributors either have a Business Continuity Plan in place or are currently working on one, while only 30% of M-Reps do.
- 82% of Manufacturers include ransomware as part of their Disaster Recovery Plan while only 59% of Distributors do.
- Just over **half** of the companies surveyed said they either have no plans to purchase or are undecided with regards to maintaining an incident response retainer.
- On average, 46% of companies have not simulated a ransomware attack as part of their recovery exercises.
- **100% of companies surveyed in our industry still have some dependency on systems that are no longer supported.**
- 67% of companies **have not** adopted a zero-trust strategy or implemented micro-segmentation in their environment. Micro-segmentation and zero-trust **will reduce** the blast radius of ransomware attacks and greatly speed up recovery times.
- Misconfigured and overprivileged access is one of the leading causes of breaches**,** **20%** of companies **have not** implemented a Privileged Access Management solution.
- **Be Prepared with:**
  - **BCP (Business Continuity Plan)**
  - **DRP (Disaster Recovery Plan)**
  - **TTE (Table-Top Exercises)**
  - **Up-to-Date Systems**
  - **Isolate Obsolete Systems**
  - **Authentication Process with Audits**
  - **Ransomware Strategy Identified**

GIPC
Cybersecurity Work Group

Our Core Team

Our core team will continue its work in 2023 with the intent to strengthen the readiness and safety of the electronic component authorized channel…

ecia
Electronic Components Industry Association