Cybersecurity
Ransomware Readiness

Survey Dates: Oct 4 – Nov 2, 2022

Dale Ford – Chief Analyst
November 8, 2022
Participant Profile – By Type

Participants by Type

- Manufacturer Representative, 23%
- Manufacturer, 39%
- Distributor, 39%

TOTAL = 44

Participants by Company Size

- Distributor: 53%
- Manufacturer: 29% 35% 29%
- Manufacturer Representative: 100%

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Tabletop Exercise Frequency - By Type

How often do you perform cyber tabletop exercises?

- Distributor:
  - Quarterly: 18%
  - Annually: 35%
  - Currently not performing: 29%
  - Other: 22%

- Manufacturer:
  - Quarterly: 18%
  - Annually: 29%
  - Currently not performing: 29%
  - Other: 24%

- Manufacturer Representative:
  - Quarterly: 0%
  - Annually: 0%
  - Currently not performing: 90%
  - Other: 10%

- Average:
  - Quarterly: 12%
  - Annually: 20%
  - Currently not performing: 52%
  - Other: 17%
Tabletop Exercise Frequency - By Size

How often do you perform cyber tabletop exercises?

- **Quarterly**
  - 50 or less: 5%
  - 51 - 500: 13%
  - 501 - 5000: 25%
  - 5001 and above: 0%
  - Average: 17%

- **Annually**
  - 50 or less: 20%
  - 51 - 500: 13%
  - 501 - 5000: 25%
  - 5001 and above: 0%
  - Average: 18%

- **Currently not performing**
  - 50 or less: 0%
  - 51 - 500: 13%
  - 501 - 5000: 13%
  - 5001 and above: 0%
  - Average: 0%

- **Other**
  - 50 or less: 75%
  - 51 - 500: 50%
  - 501 - 5000: 38%
  - 5001 and above: 88%
  - Average: 34%

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
List of “Others” for Tabletop Exercise Frequency

**Distributors**
- As incidents arise - we are 20 employee firm with 1 building so easy to pull it together periodically.
- Regular but random

**Manufacturers**
- Every other year
- As schedule as project
- We have monthly training via videos and semi annual simulations.
- Plan to begin annual testing in the next 60 days

**Manufacturer Representatives**
- Done by corporate office
On average, what is the duration of your cyber tabletop exercises?

- **Distributor**
  - Multi-day: 12%
  - Full day: 18%
  - Half day: 29%
  - < Half day: 41%
  - Currently not performing: 0%
- **Manufacturer**
  - Multi-day: 12%
  - Full day: 18%
  - Half day: 29%
  - < Half day: 24%
  - Currently not performing: 0%
- **Manufacturer Representative**
  - Multi-day: 0%
  - Full day: 0%
  - Half day: 0%
  - < Half day: 0%
  - Currently not performing: 100%
- **Average**
  - Multi-day: 8%
  - Full day: 6%
  - Half day: 16%
  - < Half day: 16%
  - Currently not performing: 55%
Tabletop Exercise Duration – By Size

On average, what is the duration of your cyber tabletop exercises?

- 50 or less: 16% Multi-day, 13% Full day, 13% Half day, 13% < Half day, 0% Currently not performing
- 51 - 500: 25% Multi-day, 13% Full day, 13% Half day, 13% < Half day, 0% Currently not performing
- 501 - 5000: 25% Multi-day, 13% Full day, 13% Half day, 13% < Half day, 0% Currently not performing
- 5001 and above: 63% Multi-day, 13% Full day, 13% Half day, 13% < Half day, 0% Currently not performing
- Average: 34% Multi-day, 13% Full day, 13% Half day, 13% < Half day, 9% Currently not performing

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
In the event of a ransomware attack, how would your company respond to demands for payment?

- **Distributor**
  - Will Never Pay: 53%
  - Depends on circumstances: 24%
  - Other: 24%

- **Manufacturer**
  - Will Never Pay: 63%
  - Depends on circumstances: 31%
  - Other: 6%

- **Manufacturer Representative**
  - Will Never Pay: 44%
  - Depends on circumstances: 22%
  - Other: 33%

- **Average**
  - Will Never Pay: 53%
  - Depends on circumstances: 26%
  - Other: 21%
In the event of a ransomware attack, how would your company respond to demands for payment?

- Will Never Pay
- Depends on circumstances
- Other

<table>
<thead>
<tr>
<th>Size</th>
<th>Will Never Pay</th>
<th>Depends on circumstances</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 or less</td>
<td>58%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>51 - 500</td>
<td>50%</td>
<td>38%</td>
<td>13%</td>
</tr>
<tr>
<td>501 - 5000</td>
<td>63%</td>
<td>25%</td>
<td>13%</td>
</tr>
<tr>
<td>5001 and above</td>
<td>43%</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td>Average</td>
<td>53%</td>
<td>28%</td>
<td>19%</td>
</tr>
</tbody>
</table>
List of “Others” for Ransomware Attack Response

Distributors
• We do not plan on paying, but I wouldn't say never
• We have insurance against ransomware
• You cannot pay and get your data back. Advanced ERP systems are broken. Have great back up database and spend your monies switching to that.
• Prefer to not state publicly

Manufacturers
• Our IRP calls for the involvement of legal on a global scale

Manufacturer Representatives
• Corporate would decide
• Refer immediately to our IT company. We had a ransomware attack, and our IT company disarmed it.
Has your company experienced any ransomware related activity?

- **Distributor**
  - No: 53%
  - Small scale/isolated incident: 18%
  - Large: 24%
  - Prefer not to answer: 6%

- **Manufacturer**
  - No: 65%
  - Small scale/isolated incident: 24%
  - Large: 12%
  - Prefer not to answer: 0%

- **Manufacturer Representative**
  - No: 70%
  - Small scale/isolated incident: 20%
  - Large: 0%
  - Prefer not to answer: 10%

- **Average**
  - No: 63%
  - Small scale/isolated incident: 20%
  - Large: 12%
  - Prefer not to answer: 5%
Has your company experienced any ransomware related activity?

- **50 or less**: 10% No, 25% Small scale/isolated incident, 13% Large, 13% Prefer not to answer
- **51 - 500**: 38% No, 25% Small scale/isolated incident, 13% Large, 13% Prefer not to answer
- **501 - 5000**: 10% No, 0% Small scale/isolated incident, 13% Large, 13% Prefer not to answer
- **5001 and above**: 0% No, 0% Small scale/isolated incident, 0% Large, 50% Prefer not to answer
- **Average**: 24% No, 15% Small scale/isolated incident, 15% Large, 4% Prefer not to answer
Do you have an updated Business Continuity Plan?

- **Distributor**: 76% Yes, 24% Currently working on a BCP, 0% Currently don’t have a BCP
- **Manufacturer**: 71% Yes, 29% Currently working on a BCP, 0% Currently don’t have a BCP
- **Manufacturer Representative**: 70% Yes, 20% Currently working on a BCP, 10% Currently don’t have a BCP
- **Average**: 56% Yes, 21% Currently working on a BCP, 23% Currently don’t have a BCP
Business Continuity Plan – By Size

Do you have an updated Business Continuity Plan?

- 50 or less: 50% Yes, 35% Currently working on a BCP, 15% Currently don’t have a BCP
- 51 - 500: 100% Yes, 0% Currently working on a BCP, 0% Currently don’t have a BCP
- 501 - 5000: 63% Yes, 38% Currently working on a BCP, 0% Currently don’t have a BCP
- 5001 and above: 100% Yes, 0% Currently working on a BCP, 0% Currently don’t have a BCP
- Average: 78% Yes, 13% Currently working on a BCP, 9% Currently don’t have a BCP

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Ransomware as Part of Disaster Recovery Exercise – By Type

Have you incorporated ransomware as part of your Disaster Recovery Exercises?

- Distributor: 59% Yes, 24% No, 18% We don’t do DREs
- Manufacturer: 82% Yes, 0% No, 0% We don’t do DREs
- Manufacturer Representative: 60% Yes, 20% No, 20% We don’t do DREs
- Average: 54% Yes, 20% No, 26% We don’t do DREs
Have you incorporated ransomware as part of your Disaster Recovery Exercises?

- **50 or less:**
  - Yes: 30%
  - No: 30%
  - We don't do DREs: 40%

- **51 - 500:**
  - Yes: 75%
  - No: 13%
  - We don't do DREs: 13%

- **501 - 5000:**
  - Yes: 88%
  - No: 13%
  - We don't do DREs: 0%

- **5001 and above:**
  - Yes: 88%
  - No: 13%
  - We don't do DREs: 0%

- **Average:**
  - Yes: 70%
  - No: 17%
  - We don't do DREs: 13%
Does your company have an Incident Response Retainer?

- **Distributor**
  - Purchased directly from an Incident Response firm: 19%
  - Currently provided through cyber insurance company: 44%
  - No plans to purchase: 13%
  - Undecided: 25%

- **Manufacturer**
  - Purchased directly from an Incident Response firm: 18%
  - Currently provided through cyber insurance company: 24%
  - No plans to purchase: 24%
  - Undecided: 35%

- **Manufacturer Representative**
  - Purchased directly from an Incident Response firm: 0%
  - Currently provided through cyber insurance company: 50%
  - No plans to purchase: 10%
  - Undecided: 40%

- **Average**
  - Purchased directly from an Incident Response firm: 12%
  - Currently provided through cyber insurance company: 26%
  - No plans to purchase: 29%
  - Undecided: 33%
Incident Response Retainer – By Size

Does your company have an Incident Response Retainer?

- **Purchased directly from an Incident Response firm**
- **Currently provided through cyber insurance company**
- **No plans to purchase**
- **Undecided**

<table>
<thead>
<tr>
<th>Size</th>
<th>Purchased</th>
<th>Provided</th>
<th>No Plans</th>
<th>Undecided</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 or less</td>
<td>25%</td>
<td>40%</td>
<td>30%</td>
<td>0%</td>
</tr>
<tr>
<td>51 - 500</td>
<td>50%</td>
<td>50%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>501 - 5000</td>
<td>43%</td>
<td>43%</td>
<td>14%</td>
<td>0%</td>
</tr>
<tr>
<td>5001 and above</td>
<td>63%</td>
<td>38%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Average</td>
<td>29%</td>
<td>21%</td>
<td>33%</td>
<td></td>
</tr>
</tbody>
</table>

Global Industry Practices Committee (GIPC)
Oldest Age of Unsupported/Legacy Technology – By Type

Oldest age of unsupported/legacy technology in your environment?

- **Distributor**
  - Less than 5 years out of support: 69%
  - Between 5 and 10 years out of support: 6%
  - Greater than 10 years out of support: 25%

- **Manufacturer**
  - Less than 5 years out of support: 50%
  - Between 5 and 10 years out of support: 25%
  - Greater than 10 years out of support: 25%

- **Manufacturer Representative**
  - Less than 5 years out of support: 70%
  - Between 5 and 10 years out of support: 20%
  - Greater than 10 years out of support: 10%

- **Average**
  - Less than 5 years out of support: 63%
  - Between 5 and 10 years out of support: 23%
  - Greater than 10 years out of support: 14%

**Global Industry Practices Committee (GIPC)**

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Oldest age of unsupported/legacy technology in your environment?

- **50 or less:**
  - Less than 5 years out of support: 70%
  - Between 5 and 10 years out of support: 25%
  - Greater than 10 years out of support: 5%

- **51 - 500:**
  - Less than 5 years out of support: 88%
  - Between 5 and 10 years out of support: 13%
  - Greater than 10 years out of support: 0%

- **501 - 5000:**
  - Less than 5 years out of support: 43%
  - Between 5 and 10 years out of support: 43%
  - Greater than 10 years out of support: 14%

- **5001 and above:**
  - Less than 5 years out of support: 57%
  - Between 5 and 10 years out of support: 29%
  - Greater than 10 years out of support: 14%

- **Average:**
  - Less than 5 years out of support: 57%
  - Between 5 and 10 years out of support: 24%
  - Greater than 10 years out of support: 19%
Please select the controls your company has implemented (Select all that apply)

- Privileged Access Management
- USB Device Management
- Network Detection and Response
- Endpoint Detection and Response
- Network Access Control
- Private Access (e.g., ZScaler, Prisma)
- Micro-segmentation
Cybersecurity Control Implementation – By Type

Please select the controls your company has implemented (Select all that apply)

Global Industry Practices Committee (GIPC)
Cybersecurity Control Implementation – By Size

Please select the controls your company has implemented (Select all that apply)

- Privileged Access Management
- USB Device Management
- Endpoint Detection and Response
- Private Access (e.g., ZScaler, Prisma)
- Network Access Control
- Micro-segmentation
- Network Detection and Response

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
<table>
<thead>
<tr>
<th>Category</th>
<th>User Behavior Analysis</th>
<th>Data Loss Prevention</th>
<th>Secure Web Browsing (Off/On Network)</th>
<th>Cloud Access Security Broker (CASB)</th>
<th>SSL Decryption</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 or less</td>
<td>11%</td>
<td>6%</td>
<td>28%</td>
<td>28%</td>
<td>28%</td>
<td>33%</td>
</tr>
<tr>
<td>51 - 500</td>
<td>25%</td>
<td>13%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>38%</td>
</tr>
<tr>
<td>501 - 5000</td>
<td>14%</td>
<td>14%</td>
<td>57%</td>
<td>57%</td>
<td>57%</td>
<td>50%</td>
</tr>
<tr>
<td>5001 and above</td>
<td>0%</td>
<td>38%</td>
<td>75%</td>
<td>75%</td>
<td>75%</td>
<td>38%</td>
</tr>
<tr>
<td>Average</td>
<td>21%</td>
<td>11%</td>
<td>49%</td>
<td>49%</td>
<td>49%</td>
<td>57%</td>
</tr>
</tbody>
</table>
List of “Others” for Cybersecurity Controls

Distributors
• Lots of Month/Week/Day/Hour Offsite roll back backups and near realtime off site data sync on Key DB Files

Manufacturers
• SIEM, PAM, MFA projects are in progress
• Currently in process of CMMC readiness
• I'm not sure if we consider it Network Detection and Response but, we employ deception or honeypotting technology also!

Manufacturer Representatives
• All web-based service products
• Corporate has responsibility