Cybersecurity

Ransomware Readiness

Survey Dates: Oct 4 – Nov 2, 2022

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

Participants by Type

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

TOTAL = 44

Participants by Company Size

- Distributor: 53%
- Manufacturer: 18% (50 or Less), 12% (51-500), 18% (501-5000)
- Manufacturer Representative: 100%

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Participant Profile – By Size

Participants by Size

- 50 or less, 45%
- 501 - 5000, 18%
- 5001 and above, 18%
- 51 - 500, 18%

TOTAL = 44

Participants by Company Size

- 50 or less: 53% Distributor, 45% Manufacturer, 100% Manufacturer Representative
- 51 - 500: 18% Distributor, 18% Manufacturer, 0% Manufacturer Representative
- 501 - 5000: 12% Distributor, 0% Manufacturer, 0% Manufacturer Representative
- 5001 and above: 18% Distributor, 18% Manufacturer, 18% Manufacturer Representative

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: 18%
  - Currently not performing: 35%

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

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

- Average:
  - Quarterly: 12%
  - Annually: 20%
  - Currently not performing: 52%
  - Other: 17%
How often do you perform cyber tabletop exercises?

- **50 or less**
  - Quarterly: 5%
  - Annually: 0%
  - Currently not performing: 20%
  - Other: 20%
- **51 - 500**
  - Quarterly: 13%
  - Annually: 13%
  - Currently not performing: 50%
  - Other: 13%
- **501 - 5000**
  - Quarterly: 25%
  - Annually: 13%
  - Currently not performing: 38%
  - Other: 25%
- **5001 and above**
  - Quarterly: 0%
  - Annually: 0%
  - Currently not performing: 88%
  - Other: 13%
- **Average**
  - Quarterly: 31%
  - Annually: 34%
  - Currently not performing: 18%
  - Other: 18%

Global Industry Practices Committee (GIPC)
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?

- Multi-day
- Full day
- Half day
- < Half day
- Currently not performing

50 or less: 16%, 13%, 13%, 13%, 0%
51 - 500: 0%, 25%, 25%, 25%, 0%
501 - 5000: 0%, 13%, 13%, 13%, 0%
5001 and above: 0%, 13%, 13%, 13%, 0%
Average: 20%, 25%, 34%, 13%, 9%

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Ransomware Attack Response – By Type

In the event of a ransomware attack, how would your company respond to demands for payment?

<table>
<thead>
<tr>
<th></th>
<th>Will Never Pay</th>
<th>Depends on circumstances</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributor</td>
<td>53%</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>63%</td>
<td>31%</td>
<td>6%</td>
</tr>
<tr>
<td>Manufacturer Representative</td>
<td>44%</td>
<td>22%</td>
<td>33%</td>
</tr>
<tr>
<td>Average</td>
<td>53%</td>
<td>26%</td>
<td>21%</td>
</tr>
</tbody>
</table>
In the event of a ransomware attack, how would your company respond to demands for payment?

- **50 or less**: 58% Will Never Pay, 21% Depends on circumstances, 21% Other
- **51 - 500**: 50% Will Never Pay, 38% Depends on circumstances, 13% Other
- **501 - 5000**: 63% Will Never Pay, 25% Depends on circumstances, 13% Other
- **5001 and above**: 43% Will Never Pay, 29% Depends on circumstances, 29% Other
- **Average**: 53% Will Never Pay, 28% Depends on circumstances, 19% Other
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.
Business Continuity Plan – By Type

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?

<table>
<thead>
<tr>
<th></th>
<th>50 or less</th>
<th>51 - 500</th>
<th>501 - 5000</th>
<th>5001 and above</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>50%</td>
<td>100%</td>
<td>63%</td>
<td>100%</td>
<td>78%</td>
</tr>
<tr>
<td>Currently working on a BCP</td>
<td>35%</td>
<td>0%</td>
<td>38%</td>
<td>0%</td>
<td>13%</td>
</tr>
<tr>
<td>Currently don’t have a BCP</td>
<td>15%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>9%</td>
</tr>
</tbody>
</table>
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, 18% 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**: 30% Yes, 40% No, 30% We don’t do DREs
- **51 - 500**: 75% Yes, 13% No, 13% We don’t do DREs
- **501 - 5000**: 88% Yes, 0% No, 13% We don’t do DREs
- **5001 and above**: 88% Yes, 0% No, 13% We don’t do DREs
- **Average**: 70% Yes, 17% No, 13% We don’t do DREs
Incident Response Retainer – By Type

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></th>
<th>Distributed</th>
<th>Manufacturer</th>
<th>Manufacturer Representative</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchased directly</td>
<td>19%</td>
<td>13%</td>
<td>44%</td>
<td>19%</td>
</tr>
<tr>
<td>Currently provided</td>
<td>18%</td>
<td>0%</td>
<td>0%</td>
<td>12%</td>
</tr>
<tr>
<td>No plans to purchase</td>
<td>25%</td>
<td>24%</td>
<td>10%</td>
<td>29%</td>
</tr>
<tr>
<td>Undecided</td>
<td>24%</td>
<td>40%</td>
<td>50%</td>
<td>33%</td>
</tr>
</tbody>
</table>
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

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
Oldest Age of Unsupported/Legacy Technology – By Type

Oldest age of unsupported/legacy technology in your environment?

- Distributor: 69% (Less than 5 years out of support), 25% (Between 5 and 10 years out of support), 6% (Greater than 10 years out of support)
- Manufacturer: 50% (Less than 5 years out of support), 25% (Between 5 and 10 years out of support), 25% (Greater than 10 years out of support)
- Manufacturer Representative: 70% (Less than 5 years out of support), 20% (Between 5 and 10 years out of support), 10% (Greater than 10 years out of support)
- Average: 63% (Less than 5 years out of support), 23% (Between 5 and 10 years out of support), 14% (Greater than 10 years out of support)
Oldest Age of Unsupported/Legacy Technology – By Size

Oldest age of unsupported/legacy technology in your environment?

- Less than 5 years out of support
- Between 5 and 10 years out of support
- Greater than 10 years out of support

- 50 or less: 70% (25% less than 5 years, 5% 51-500), 25% (5% less than 5 years, 20% 51-500), 14% (14% less than 5 years, 14% 51-500)
- 51-500: 88% (13% less than 5 years, 0% 51-500), 43% (14% less than 5 years, 29% 51-500), 29% (14% less than 5 years, 14% 51-500)
- 501-5000: 43% (14% less than 5 years, 29% 51-500), 14% (14% less than 5 years, 14% 51-500), 14% (14% less than 5 years, 14% 51-500)
- 5001 and above: 57% (29% less than 5 years, 57% 51-500), 57% (29% less than 5 years, 57% 51-500), 57% (29% less than 5 years, 57% 51-500)

Average: 24% (19% less than 5 years, 29% 51-500), 24% (19% less than 5 years, 29% 51-500), 24% (19% less than 5 years, 29% 51-500)
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

Distributor: 93% Privileged Access Management, 87% USB Device Management, 73% Network Detection and Response
Manufacturer: 82% Privileged Access Management, 82% USB Device Management, 76% Network Detection and Response
Manufacturer Representative: 53% Privileged Access Management, 41% USB Device Management, 47% Network Detection and Response
Average: 70% Privileged Access Management, 60% USB Device Management, 62% Network Detection and Response

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
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

Global Industry Practices Committee (GIPC)

© Copyright 2020 Electronic Components Industry Association. All rights reserved.
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