Cybersecurity

August 2021
Research Overview

HIMSS Market Intelligence conducted this research in May to June 2021. The research was conducted among medical IT practitioners to understand cybersecurity awareness in a hospital / health system setting. Topics included:

• Gauging baseline for security awareness
• Cybersecurity training
• Cybersecurity budgets and allocations
• Understanding what healthcare cybersecurity professionals are most concerned about

Methodology

• This research was conducted online amongst IT practitioner leaders in healthcare in the United States.
• Respondents were screened for working in a relevant function (IT / Technology, IT security / Cybersecurity or Executive Leadership) and for having a role in decision making regarding cybersecurity at their organization.
• A total of 250 qualified respondents participated in this research.
• This was a blind data collection effort, Auth0 was not identified as a sponsor of the research.
Detailed Findings
3-in-4 are concerned about the possibility of a security breach on their organization’s network connected medical devices

Tell us your level of concern when thinking of your organization’s network connected medical devices and the possibility of a security breach

On a scale of 1-5 where 1=Not at all concerned and 5=Extremely concerned, please tell us your level of concern when thinking of your organization’s network connected medical devices and the possibility of a security breach i.e.: a security attack. Base: Total Respondents: n=250

- (5) Extremely concerned: 22%
- (4): 54%
- (3): 18%
- (2): 7%
- (1) Not at all concerned: 5%

76% of participants are concerned about the possibility of a security breach

Data labels under 5% not shown
The staff at organizations is seen as the biggest cybersecurity vulnerability

What do you perceive as the biggest cybersecurity vulnerability at your organization?

- Our staff: 40%
- Networks: 24%
- Legacy systems: 14%
- Medical devices: 12%
- Cloud resources: 7%
- Industrial control systems: 2%
- Another vulnerability: 1%

Base: Total respondents; n=250
Although, 7-in-10 only saw a budget increase of 20% or less

Estimate the percent your budget has increased/decreased in the last 12 months.

Of those that confirmed they had an increase or decrease in budget, the majority stated an increase in the cybersecurity budget occurred. 95% v. 5%
With the largest percent of the cybersecurity budgets being invested in maintaining / upgrading existing infrastructure

By percentage, please tell us, on average, the relative cybersecurity budget allocation for...?

- Maintaining existing infrastructure: 17% 0-19%, 43% 20-39%, 27% 40-59%, 10% 60-79%, 0% 80-100%
  *Average: 33.09%

- Upgrading existing infrastructure: 22% 0-19%, 55% 20-39%, 18% 40-59%, 4% 60-79%, 0% 80-100%
  *Average: 27.85%

- Outsourcing cybersecurity functions: 59% 0-19%, 34% 20-39%, 4% 40-59%, 0% 60-79%, 0% 80-100%
  *Average: 15.64%

- Training staff: 58% 0-19%, 35% 20-39%, 4% 40-59%, 0% 60-79%, 0% 80-100%
  *Average: 16.66%

- Another cybersecurity budget allocation: 82% 0-19%, 14% 20-39%, 0% 40-59%, 0% 60-79%, 0% 80-100%
  *Average: 6.76%

Base: Total Respondents; n=250

Data labels under 4% not shown
Only 1-in-4 currently have a different cybersecurity budget allocation for IT and IoMT/IoT

My organization has the…

76% Same cybersecurity budget allocation for IT and IoMT/IoT

24% Different cybersecurity budget allocations for IT and IoMT/IoT
Only 1-in-2 have encryption for archived files/data, anti-theft devices, digital forensics or a business continuity/disaster recovery plan enabled for employees.

### Who are these technologies enabled for?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Employees</th>
<th>Patients</th>
<th>Both – Employees &amp; Patients</th>
<th>Unsure/I don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile device management</td>
<td>73%</td>
<td></td>
<td></td>
<td>25%</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>61%</td>
<td></td>
<td></td>
<td>33%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>58%</td>
<td>11%</td>
<td></td>
<td>28%</td>
</tr>
<tr>
<td>Vulnerability scans</td>
<td>58%</td>
<td></td>
<td></td>
<td>38%</td>
</tr>
<tr>
<td>Business continuity and disaster recovery plan</td>
<td>55%</td>
<td></td>
<td></td>
<td>43%</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>54%</td>
<td></td>
<td></td>
<td>38%</td>
</tr>
<tr>
<td>Anti-theft devices</td>
<td>54%</td>
<td></td>
<td></td>
<td>43%</td>
</tr>
<tr>
<td>Encryption for archived files/data</td>
<td>50%</td>
<td></td>
<td></td>
<td>27%</td>
</tr>
</tbody>
</table>

And, who are these technologies enabled for?

Base: Technologies currently in place to implement; Biometrics n=101, Digital forensics n=101, Penetration testing n=142, Vulnerability scans n=199, Anti-theft devices n=148, Business continuity and disaster recovery plan n=187, Mobile device mgmt n=194, Encryption for archived files/data n=208. Other n=2

Data labels under 5% & “Other” not shown
The majority (93%) are conducting cybersecurity training within their organization and those with a net revenue of ≥$5.1B, having 100% currently training on cybersecurity. On average, cybersecurity training is occurring at least quarterly (75%). While the majority of Non-IT staff (80%-82%) are being trained, vendors (28%) are not.

Staff is seen as the biggest cybersecurity vulnerability

The majority (93%) are conducting cybersecurity training within their organization and those with a net revenue of ≥$5.1B, having 100% currently training on cybersecurity. On average, cybersecurity training is occurring at least quarterly (75%). While the majority of Non-IT staff (80%-82%) are being trained, vendors (28%) are not.

Nearly 7-in-10 have seen an increase in their cybersecurity budget in the last 12 months

Majority (82%) only seeing an increase of 20% or less. The largest percent of the cybersecurity budget being invested in maintaining (33%) and upgrading (28%) existing infrastructure. Not many have a different cybersecurity budget allocations for IT and IoMT/IoT (24%). HIPAA violations (87%) and patient safety (82%) are top of mind as cybersecurity budgets are created.

Only half have security technologies in place for their employees

Although staff is deemed to be the biggest cyber security vulnerability, encryption for archived files/data (50%), anti-theft devices (54%), digital forensics (54%) or a business continuity/disaster recovery plan (55%) is stated to only be enabled for employees at half of the organizations. Nearly a third are planning to implement biometrics (29%), digital forensics (28%), or penetration testing (28%) within the next 24 months. With larger organizations (28% at a net rev. of $1.1B-$5B; 32% at a net rev. of ≥$5.1B) significantly more likely to implement biometrics in less than 12 months.

Key Takeaways

1. 3-in-4 are concerned about the possibility of a security breach
   Over 60% of organizations have a CISO (67%) and/or use cyber liability insurance (63%). The majority (93%) with a net revenue of ≥$5.1B, have a CISO.

2. Staff is seen as the biggest cybersecurity vulnerability
   The majority (93%) are conducting cybersecurity training within their organization and those with a net revenue of ≥$5.1B, having 100% currently training on cybersecurity. On average, cybersecurity training is occurring at least quarterly (75%). While the majority of Non-IT staff (80%-82%) are being trained, vendors (28%) are not.

3. Nearly 7-in-10 have seen an increase in their cybersecurity budget in the last 12 months
   Majority (82%) only seeing an increase of 20% or less. The largest percent of the cybersecurity budget being invested in maintaining (33%) and upgrading (28%) existing infrastructure. Not many have a different cybersecurity budget allocations for IT and IoMT/IoT (24%). HIPAA violations (87%) and patient safety (82%) are top of mind as cybersecurity budgets are created.

4. Only half have security technologies in place for their employees
   Although staff is deemed to be the biggest cyber security vulnerability, encryption for archived files/data (50%), anti-theft devices (54%), digital forensics (54%) or a business continuity/disaster recovery plan (55%) is stated to only be enabled for employees at half of the organizations. Nearly a third are planning to implement biometrics (29%), digital forensics (28%), or penetration testing (28%) within the next 24 months. With larger organizations (28% at a net rev. of $1.1B-$5B; 32% at a net rev. of ≥$5.1B) significantly more likely to implement biometrics in less than 12 months.
Thank You

For more information please contact:

**Stephen Wellman**
Market Intelligence Manager
Stephen.Wellman@himss.org