



COMMUNITY
HEALTH CARE
ASSOCIATION
of New York State

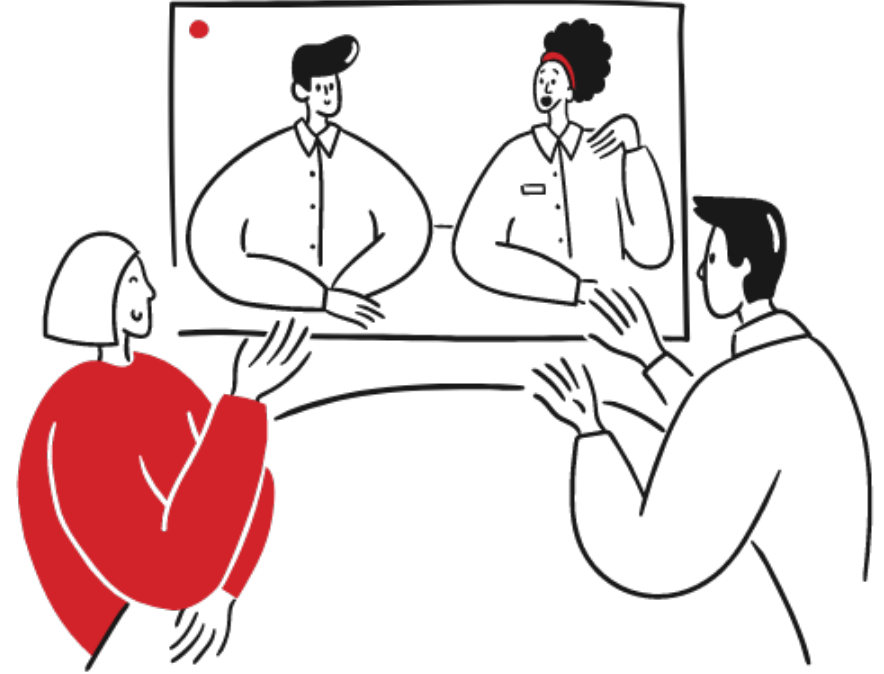
CHCANYS NYS-HCCN presents a four-part learning series with Online Business Systems

Prioritizing Security Enhancements: Putting Cyber Resources into Action

**Session 2
January 25, 2023**

Zoom Guidelines

- You have been muted upon entry. Please respect our presenters and stay on mute if you are not speaking.
- Please share your questions in the chat. CHCANYS staff will raise your questions to our speakers and follow up as needed if there are unanswered questions.
- The workshop is being recorded and slides will be shared after the session.



New York State HCCN Objectives



Project Period 2022-2025

1 **Clinical Quality**

2 **Patient-Centered Care**

3 **Provider and Staff Wellbeing**

2022-2025 Project Period

- ✓ Patient Engagement
- ✓ Patient Privacy & Cybersecurity
- ✓ Social Risk Factor Intervention
- ✓ Disaggregated Patient-level Data (UDS+)
- ✓ Interoperable Data Exchange & Integration
- ✓ Data Utilization
- ✓ Leveraging Digital Health Tools
- ✓ Health IT Usability & Adoption
- ✓ Health Equity and REaL Data Collection*
- ✓ Improving Digital Health Tools- Closed Loop Referrals*

* - Applicant Choice Objective
Bold- Objective Carried over into 2022-2025



Prioritizing Security Enhancements



Adam Kehler, CISSP

Director of RSP Healthcare Service

Online Business Systems





Session 2: Putting Cyber Resources into Action!

Prioritizing Security Enhancements

Objectives

❖ Risk Management

❖ Prioritizing Security Enhancements

❖ Implementing Security Enhancements

❖ Budgeting for Cybersecurity

Problem Statement

We know we have to improve our cybersecurity posture, but we can't do everything with limited budget and resources. How do we prioritize and what happens if we don't do everything?

Goals


What are your goals?

1. Protect Patient Information?
2. Comply with HIPAA?
3. Avoid regulatory fines and corrective action plans?
4. Meet requirements of cyber insurance?
5. Reduce financial risk to the organization

Problem Statement #2

"When CIOs gear up to speak about IT priorities in the annual board meeting, they may as well be speaking a different language."

<https://www.ciodive.com/news/MIT-sloan-CIO-symposium-communicating-IT-board-members/599997/>

 Results. Guaranteed.

Risk Management

Compliance vs. Security



HIPAA and Risk Management

Standard 164.308(a)(1)(i), *Security Management Process*, requires regulated entities to:

Implement policies and procedures to prevent, detect, contain, and correct security violations.

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management:

1. **Risk Analysis (R¹⁴)** – 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
2. **Risk Management (R)** – 163.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

Security Risk Analysis

- Does your SRA provide a list of gaps or a list of risks?

Gap

The organization does not have Multi-Factor Authentication in place.

The organization does not have network segmentation.

Risk

There is a high likelihood that a phishing attack would succeed due to the absence of MFA and network segmentation. This could result in attackers gaining access to the local network and pivoting to critical systems such as the EMR resulting in loss of data, a large breach, or loss of services.

Assessment/Analysis Approach



The Security Risk Assessment approach is designed to allow organizations to implement "reasonable and appropriate" security controls as opposed to being prescriptive



For example, what is a reasonable disaster recovery plan for a large health system would be excessive for a small doctor's office; this allows flexibility while still being enforceable



If other organizations of the same size are encrypting their laptops, it would seem reasonable to expect your organization to do the same



But how can you determine what is "reasonable and appropriate" for your organization?

Take a Security Risk Management approach and look to industry standards and guidance



 Results. Guaranteed.

Prioritizing Security Enhancements

Goals

What are your goals?

1. Protect Patient Information? 405(d)/NIST CSF
2. Comply with HIPAA? Risk Analysis, Risk Management
3. Avoid regulatory fines and corrective action plans? Risk Analysis, Risk Management, 405(d)/NIST CSF
4. Meet requirements of cyber insurance? Implement specific controls
5. Reduce financial risk to the organization Do #1-#4

Cyber Insurance Underwriting Standards

- Multifactor Authentication (MFA)
 - All remote access (both employee and third party)
 - All privileged user accounts, including when on prem
 - Access to remote desktop protocol (RDP)
 - Access to cloud/hosted/SaaS solutions
 - Access to backups
 - Some carriers are now asking for the type of MFA used
- Endpoint detection and response (EDR) products
- Liberal granting of local administrative rights
- Patching cadence, specifically for critical and high/important severity patches
- End-of-life software and compensating controls
- Backups
 - MFA
 - Separate credentials
 - Rapid RPOs and short RTOs
 - Encryption
 - Offline or immutable
 - Testing of restoration/recovery E6M or E12M
 - Ability to test integrity

Cyber Insurance Underwriting Standards

- External email tagging
- SPF, DKIM, DMARC
- Use of O365 ATP or similar
- Privileged Account Management (PAM) tool
- Security Operations Center (SOC)
- Minimal service accounts in domain admin group

Prioritizing Security Enhancements

| | | Impact → | | | | |
|--------------|---------------|------------|----------|----------|-------------|----------|
| | | Negligible | Minor | Moderate | Significant | Severe |
| Likelihood ↑ | Very Likely | Low | Moderate | High | High | High |
| | Likely | Low | Moderate | Moderate | High | High |
| | Possible | Low | Low | Moderate | Moderate | High |
| | Unlikely | Low | Low | Moderate | Moderate | Moderate |
| | Very Unlikely | Low | Low | Low | Moderate | Moderate |

Prioritizing Security Enhancements

- With risks in hand, translate to organizational risk
- Executives are good at making risk-based decisions
- Which makes it easier for a CFO or CEO to make a decision:
 - “We need \$20,000 to implement MFA and network segmentation. MFA will make people take extra steps to login to our systems and network segmentation will increase the amount of time we’ll need from our network management contractor.”
 - “There is an extremely high likelihood that Phishing/Ransomware will affect our EMR server. If this happens, we may have to pay a hefty ransom, go through an OCR audit, pay fines, or lose all of our patient data. We can greatly reduce this risk by implementing MFA and network segmentation which will cost \$20,000.”
- Result: Executives own the risk

Prioritizing Security Enhancements

- Examples
 1. You have a static website hosted on a website hosting service. It has vulnerabilities, isn't monitored, and doesn't require MFA on the admin portal.
 - Likelihood? Impact? Overall Risk? Priority?
 2. Your EMR system is in a dedicated network segment, requires VPN to access, has intrusion detection systems and strong physical safeguards. Your CEO is worried about it getting breached and wants to hire an MSP to manage it.
 - Likelihood? Impact? Over Risk? Priority?
 3. Your patient portal has a critical vulnerability that is being actively exploited by attackers.
 - Likelihood? Impact? Over Risk? Priority?

| | | Impact → | | | | |
|--------------|---------------|------------|----------|----------|-------------|----------|
| | | Negligible | Minor | Moderate | Significant | Severe |
| Likelihood ↑ | Very Likely | Low | Moderate | High | High | High |
| | Likely | Low | Moderate | Moderate | High | High |
| | Possible | Low | Low | Moderate | Moderate | High |
| | Unlikely | Low | Low | Moderate | Moderate | Moderate |
| | Very Unlikely | Low | Low | Low | Moderate | Moderate |




Prioritizing Security Enhancements

| Risk | Recommendations | Risk | Cost |
|---------------------------------|---|----------|----------|
| Ransomware affecting EMR System | Engage MSP | Moderate | \$20,000 |
| Attackers breaching website | Work with developer to fix holes, MFA on portal, possibly move to another platform. | Low | \$8,000 |
| Patient Portal vulnerabilities | Work with vendor to patch | High | \$4,000 |

Putting Security Into Action

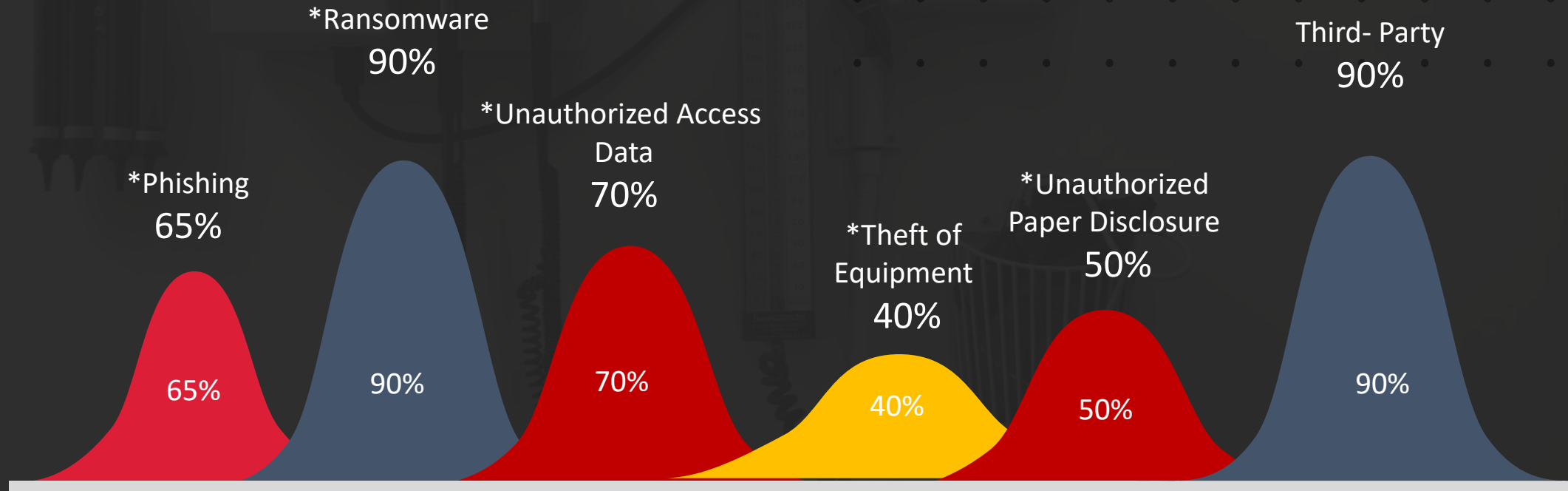
- With risks in hand, translate to organizational risk
- Executives are good at making risk-based decisions
- Which makes it easier for a CFO or CEO to make a risk-based decision:
 - “We need \$20,000 to implement MFA and network segmentation. MFA will make people take extra steps to login to our systems and network segmentation will increase the amount of time we’ll need from our network management contractor.”
 - “There is an extremely high likelihood that Phishing/Ransomware will affect our EMR server. If this happens, we may have to pay a hefty ransom, go through an OCR audit, pay fines, or lose all of our patient data. We can greatly reduce this risk by implementing MFA and network segmentation which will cost \$20,000.”

Prioritizing Security Enhancements

1. Does this approach comply with HIPAA? 
2. Does this approach increase security? 
3. Does this approach optimize use of security dollars? 
4. If you DON'T implement security controls, who owns the risk?

What Next / Putting Security into Action

FQHC Threat Results from 2020 to 2022 HIPAA SRAs



FQHC Threat Results from 2020 and 2022 SRA

*Align with 405(d) HHS Managing Threats (HICP)

| | Best Fit | Small | Medium | Large |
|---------------------|--------------------------------------|---|--|---|
| Common Attributes | Health information exchange partners | One or two partners | Several exchange partners | Significant number of partners or partners with less rigorous standards or requirements Global data exchange |
| | IT capability | No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by-project-basis | Dedicated IT resources on staff No or limited dedicated security resources on staff | Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff |
| | Cybersecurity investment | Nonexistent or limited funding | Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended | Dedicated budget with strategic roadmap specific to cybersecurity |
| Provider Attributes | Size (provider) | 1–10 physicians | 11–50 physicians | Over 50 physicians |
| | Size (acute / post-acute) | 1–25 providers | 26–500 providers | Over 500 providers |
| | Size (hospital) ¹⁵ | 1–50 beds | 51–299 beds | Over 300 beds |
| | Complexity | Single practice or care site | Multiple sites in extended geographic area | Integrated delivery networks Participate in accountable care organization or clinically integrated network |
| Other Org Types | | Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations | Health Plan Large Device Manufacturer Large pharmaceutical organization | |

Table 1. Selecting the “Best Fit” For Your Organization

| | Best Fit | Small | Medium | Large |
|---------------------|--------------------------------------|---|---|---|
| Common Attributes | Health information exchange partners | One or two partners | Several exchange partners | Significant number of partners or partners with less rigorous standards or requirements Global data exchange |
| | IT capability | No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis | Dedicated IT resources on staff No or limited dedicated security resources on staff | Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff |
| | Cybersecurity investment | Nonexistent or limited funding | Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended | Dedicated budget with strategic roadmap specific to cybersecurity |
| Provider Attributes | Size (provider) | 1–10 physicians | 11–50 physicians | Over 50 physicians |
| | Size (acute / post-acute) | 1–25 providers | 26–500 providers | Over 500 providers |
| | Size (hospital) ¹⁵ | 1–50 beds | 51–299 beds | Over 300 beds |
| | Complexity | Single practice or care site | Multiple sites in extended geographic area | Integrated delivery networks Participate in accountable care organization or clinically integrated network |
| Other Org Types | | | Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations | Health Plan Large Device Manufacturer Large pharmaceutical organization |

Table 1. Selecting the “Best Fit” For Your Organization

 Results. Guaranteed.

Demo: 405(d) Toolkit

[405\(d\) Cybersecurity Practices Assessment Toolkit](#)

405(d) HHS Managing Threats (HICP) Example

Results. Guaranteed.

- Incident Response (S)
 - Establish and implement an incident response plan
 - ISAC/ISAO Participation

| | | |
|--------------|--------------------------|---------------------------------------|
| 8.S.A | Incident Response | NIST FRAMEWORK REF: PR.IP-9 |
|--------------|--------------------------|---------------------------------------|

Table 7. Incident Response Recommendations to Mitigate Risk of a Data Breach

| Incident | Response Recommendation |
|-----------------|---|
| Malware | <ul style="list-style-type: none"> Re-image, rebuild, or reset computer to a known good state. Do not trust “malware cleaning” tools until they are verified to function as described. |
| Phishing | <ul style="list-style-type: none"> Identify malicious e-mail messages and delete from mailboxes. Proactively block websites (URLs) referenced in “click attacks.” Identify malware that might have been installed on computers, and remediate appropriately if present |

| | | |
|--------------|--------------------------------|--------------------------------|
| 8.S.B | ISAC/ISAO Participation | NIST: DETECT ID.RA-2 |
|--------------|--------------------------------|--------------------------------|

405(d) HHS Managing Threats (HICP) Example

Results. Guaranteed.

- Basic Email Protection Controls (M)

M365 Outbound Spam Policies

Table 1. E-mail Protection Controls

| Control | Description |
|--|---|
| Real-time blackhole list ³ | Community-based lists of IP addresses and host names of known or potential spam originators. Consider Spamhaus, Spamcop, DNSRBL, or lists provided by your e-mail vendor. |
| Distributed checksum clearinghouse (DCC) | The DCC is a distributed database that contains a checksum of messages. E-mail messages go through a checksum algorithm and then checked against the database. Depending upon the threshold of checksum matches, these can be determined to be spam or malicious messages. |
| Removal of open relays | Open relays are Simple Mail Transfer Protocol (SMTP) servers that enable the relay of third-party messages. SMTP is critical for the delivery of messages, but you must configure it to allow messages only from trusted sources. Failure to do this may permit a spammer or hacker to exploit the “trust” of your mail server to transmit malicious content. |
| Spam/virus check on outbound messages | Spam/virus checks on outbound e-mails can detect malicious content, revealing compromised accounts and potential security incidents. Review e-mail spam/virus rules as part of Cybersecurity Practice #8: Security Operations Center and Incident Response . |
| AV check | Scan all e-mail content against an AV engine with up-to-date signatures. If possible, this control should unpack compressed files (such as zip files) to check for embedded malware. |

405(d) HHS Managing Threats (HICP) Example

 Results. Guaranteed.

- Basic Email Protection Controls (M)

| Control | Description |
|--|---|
| Restrict the “Send !s” permission for distribution lists | Limit distribution lists to essential members. Distribution lists can enable attackers to disseminate malicious content from a compromised account. Therefore, they and should not be accessible to large numbers of users. |
| Implement sender policy framework (SPF) records | A Sender Policy Framework (SPF) record identifies which mail servers may send e-mail on behalf of your domain. This enables the receiving mail server to verify the authenticity of the sending mail server. |
| Implement domain key identified mail (DKIM) | DKIM is a method of e-mail authentication that uses cryptography to ensure that e-mail messages come from authorized e-mail servers. A public key is stored within the organization’s DNS as a text (txt) record. All messages sent from that domain are digitally signed with a DKIM signature that can be validated through the DNS public key txt record. |
| Implement domain-based message authentication reporting and conformance (DMARC)⁴ | DMARC is an authentication technology that leverages both SPF and DKIM to validate an e-mail’s <i>From:</i> address (i.e., the sender). DMARC enables the receiving mail system to check SPF and DKIM records, ensuring conformance to the sending host as well as the <i>From:</i> address. It instills trust that the sending party’s e-mail address is not spoofed; spoofing is a common attack type used to trick users into opening malicious e-mails. |

405(d) HHS Managing Threats (HICP) Example

 Results. Guaranteed.

- Vulnerability Management (M)

Cybersecurity Practice 7: Vulnerability Management

Data that may
be affected

PHI

Medium Sub-
Practices

7.M.A

Host/Server Based Scanning

7.M.B

Web Application Scanning

7.M.C

System Placement and Data Classification

7.M.D

Patch Management, Configuration
Management & Change Management

Large Sub-
Practices

7.LA

Penetration Testing

7.LB

Remediation Planning

Key Mitigated
Risks

- Ransomware Attacks
- Insider, Accidental or Intentional Data Loss
- Attacks Against Connected Medical Devices that May Affect Patient Safety

405(d) HHS Managing Threats (HICP) Example

 Results. Guaranteed.

Vulnerability Management

- Penetration Tests – fall under large org; investment often spent better elsewhere
- Vulnerability Scans – External vs Internal, Credentialed vs Uncredentialed
 - Put on an automated schedule. Automated external scan every week? Why not?
- Patching
 - At least monthly except more often when a critical vulnerability is announced.
 - Depends on several factors:
 - Exposure (external vs internal, network segmentation)
 - Criticality of asset
 - Ease of exploitability
 - Is it being actively exploited

405(d) HHS Managing Threats (HICP) Example

 Results. Guaranteed.

Table 8. Recommended Timeframes for Mitigating IT Vulnerabilities

| Vulnerability Criticality | Days to Mitigate in DMZ | Days to Mitigate in Data Center |
|---------------------------|-------------------------|---------------------------------|
| Critical | < 14 days | < 30 days |
| High | < 30 days | < 90 days |
| Medium | < 90 day | < 180 days |
| Low | < 180 days | At your discretion |




 Results. Guaranteed.

Budgeting for Cybersecurity

*2021 HIMSS Healthcare
Cybersecurity Survey*

<https://www.himss.org/resources/himss-healthcare-cybersecurity-survey>

Cybersecurity budgets:

-  **Overall, budgets are still tight.** Six percent or less of the information technology budget is typically allocated for cybersecurity.
-  **Increases in budget for some.** Cybersecurity budgets are modestly increasing compared to the previous year. But tight budgets still mean that one has to pick and choose which security solutions to acquire or implement.
-  **Decreases in budget for others.** Cybersecurity budgets are decreasing for a few. This leads to less robust cybersecurity programs as a whole.

Cybersecurity budgets:




-  **Overall, budgets are still tight.** Six percent or less of the information technology budget is typically allocated for cybersecurity.
-  **Increases in budget for some.** Cybersecurity budgets are modestly increasing compared to the previous year. But tight budgets still mean that one has to pick and choose which security solutions to acquire or implement.
-  **Decreases in budget for others.** Cybersecurity budgets are decreasing for a few. This leads to less robust cybersecurity programs as a whole.

Figure 9: Percent of Organization's IT Budget Allocated to Cybersecurity for 2021

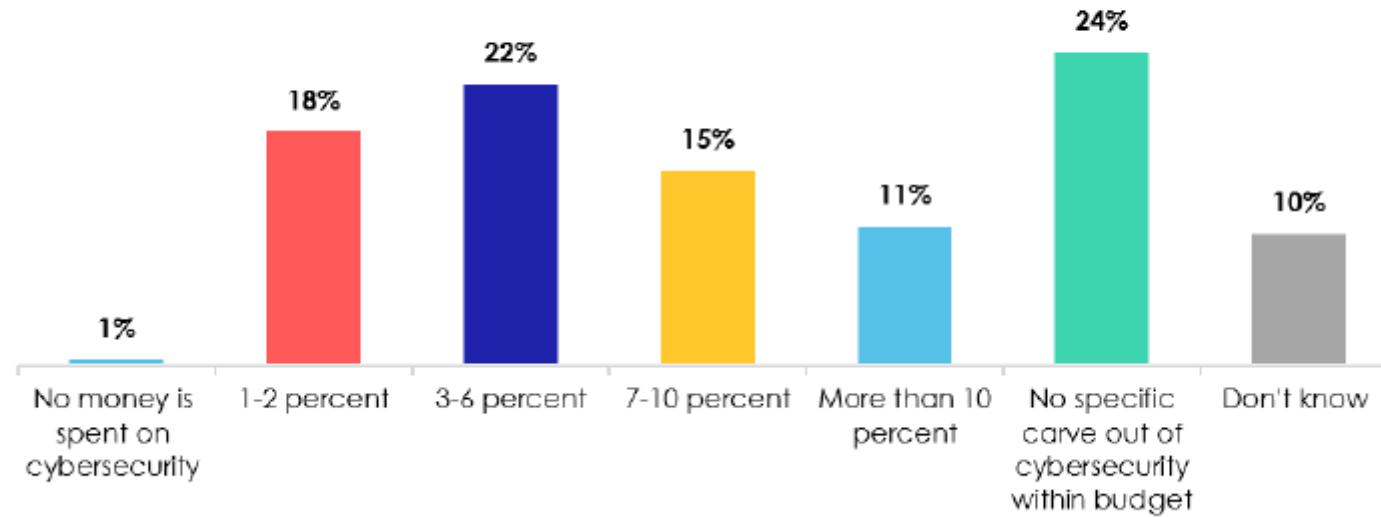


Table 3: Impact of Cybersecurity Budget Increases - 2020 to 2021

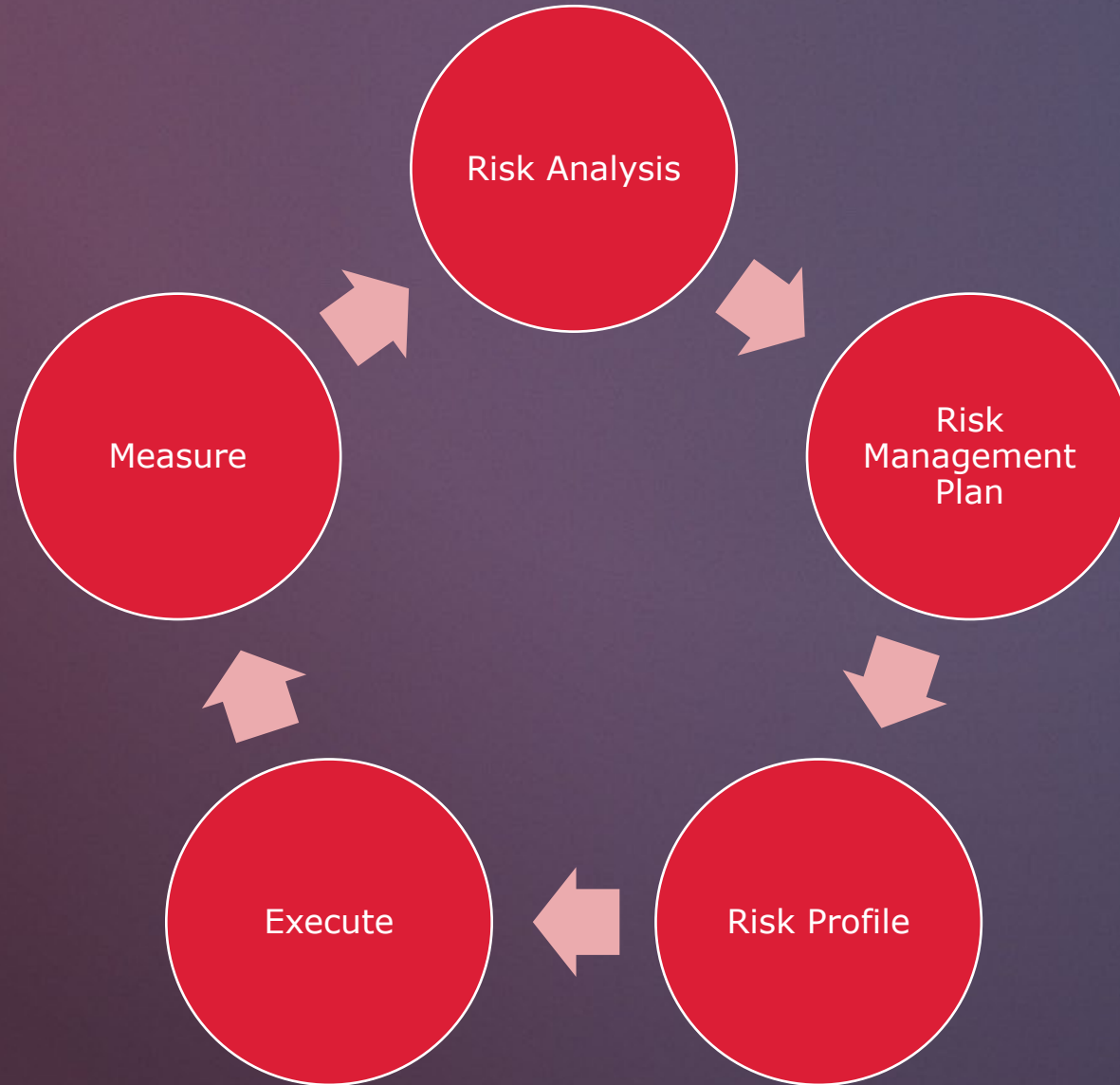
| Outcomes | Percentage |
|--|------------|
| More upgrades of security solutions | 63% |
| More acquisitions of new security solutions | 56% |
| Increase in cybersecurity staffing | 53% |
| More maintenance of existing infrastructure | 48% |
| More security risk assessments or more comprehensive security risk assessments | 48% |
| More robust security risk management | 47% |
| Increased security awareness training | 34% |
| More frequent penetration testing | 31% |
| Increased cybersecurity training for IT & IT security staff | 28% |
| Other (please specify) | 2% |

Table 4: Impact of Cybersecurity Budget Decreases 2020 to 2021

| Outcomes | Percentage |
|--|------------|
| Less acquisition of new security solutions | 67% |
| Less robust security risk management | 67% |
| Decrease in cybersecurity staffing | 50% |
| Less maintenance of existing infrastructure | 50% |
| Less cybersecurity training for IT & IT security staff | 33% |
| Fewer upgrades of security solutions | 17% |
| Fewer security risk assessments or less comprehensive risk assessments | 17% |
| Less security awareness training | 17% |
| Less frequent penetration testing | 17% |

 Results. Guaranteed.

Putting it all Together



Putting it all Together

- Learn to speak to executive-speak and risk
- Prioritized based on impact
- Select “reasonable” security controls
- Measure and re-evaluate
- Compare your budget and priorities to your peers

The background of the slide is a dark, blurred image showing several pairs of hands shaking, suggesting a meeting or agreement. A horizontal red bar spans across the middle of the image, containing the text.

Thank You

Questions?



Next Cybersecurity Session:

Best Security Practices for Partnering with Third Party Vendors

Wednesday, February 15, 12-130PM

[Register for Session 3 Here](#)

Cybersecurity Insurance:

Ask the Experts: Cybersecurity Insurance 101 (with Founder Shield)

Tomorrow, January 26, 12-1PM

[Register for Session Here](#)



Workshop Evaluation Survey

Please share your feedback on this session. This should take less than 3 minutes to complete.

Survey Link:

https://forms.office.com/Pages/ResponsePage.aspx?id=YSZI7iDhjEqs_ICzVbYzoqmlH89zfFNPhDWTC9uAhXZUM0xGUjk0QkIDSEg5R0xFR1E2WDBJUIFBQS4u



Thank you!

