Crowe

Smart decisions. Lasting value.™

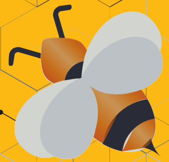
Crowe Healthcare Summit 2019

Nurture Your Network Upskill. Connect. Grow.

Top IT Risks That Could Jeopardize Your Organization

September 18

Presented by:
James Kernen
Alex Hiznay



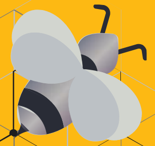
Introducing Healthcare's Trusted Community:

The Crowe Hive Network

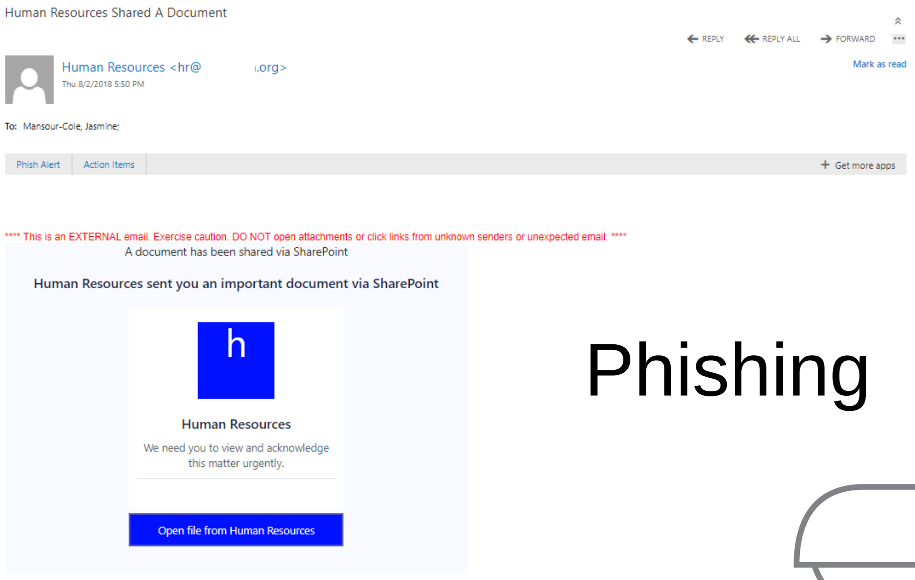
Being successful in your role today looks different than it did even a few years ago. **Engage with a network of those who have been there before you:**

- Ask and answer community questions
- Seek validation and gain support through crowdsourcing
- Connect with peers and Crowe specialists
- Earn rewards for your engagement and shop the Hive store

Simplify your busy workday. Register today to continue the Healthcare Summit conversations: **crowehive.com**.



What are some examples of IT risks?



Human Resources Shared A Document

Human Resources <hr@ .org>
Thu 8/2/2018 5:50 PM

To: Mansour-Cole, Jasmine;

**** This is an EXTERNAL email. Exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email. ****

A document has been shared via SharePoint

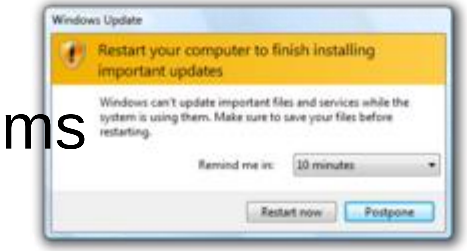
Human Resources sent you an important document via SharePoint

Human Resources

We need you to view and acknowledge this matter urgently.

Phishing

Unpatched systems



Windows Update

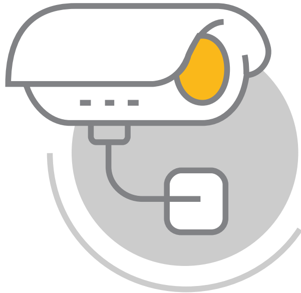
Restart your computer to finish installing important updates

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in: 10 minutes

Malware

Unauthorized access



Patient records are unavailable

Unmonitored activity

Crowe

Introductions

James Kernen

With Crowe for over 4 years, and has over 25 years experience with performing corporate governance and risk management functions, financial audits, and information systems and security assessments and program implementations.

Alex Hiznay

Over 3 years experience at Crowe, performing IT risk and compliance assessments using various control frameworks including the NIST Cybersecurity Framework (CSF), NIST 800-53, ISO 27001/2, and HIPAA.

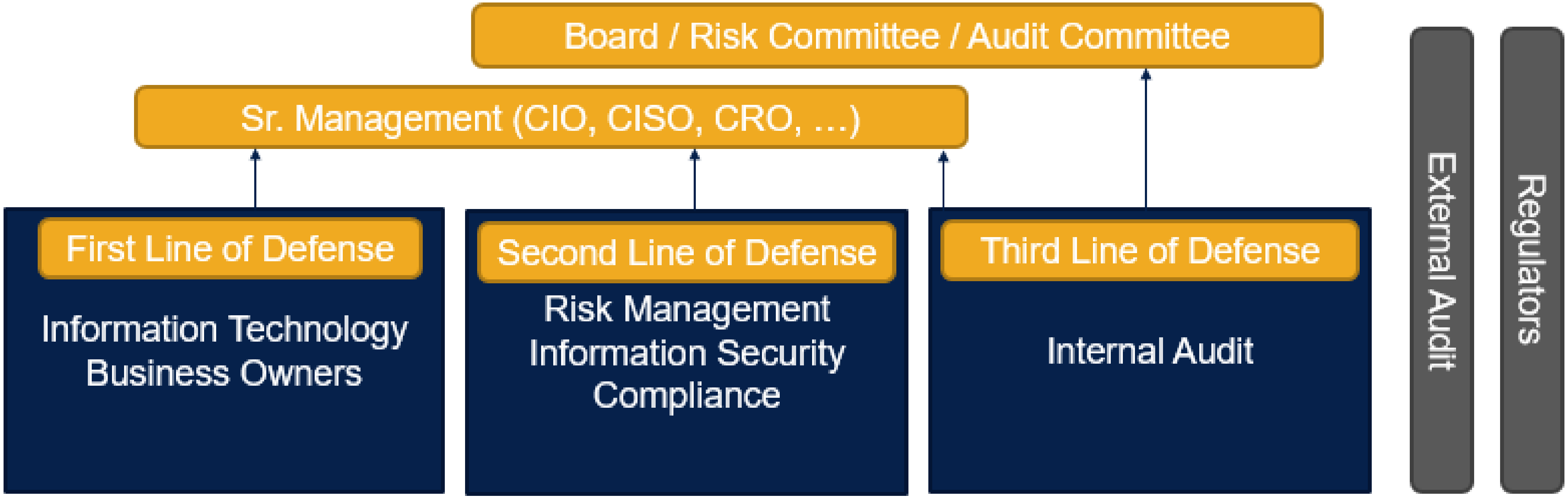
- Effective Governance and Risk Management
- Top Risk #1 – Phishing
- Top Risk #2 – User Access & Authentication
- Top Risk #3 – Mobile & Biomedical Devices
- Top Risk #4 – Business Continuity

Using Effective Governance to Manage IT Risks

What is Governance?

- The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles, and procedures the organization uses to make those decisions. (Definition by (ISC)^2)

What does Effective IT Governance Look Like?



Board / Risk Committee / Audit Committee

Sr. Management (CIO, CISO, CRO, …)

First Line of Defense

Information Technology
Business Owners

Second Line of Defense

Risk Management
Information Security
Compliance

Third Line of Defense

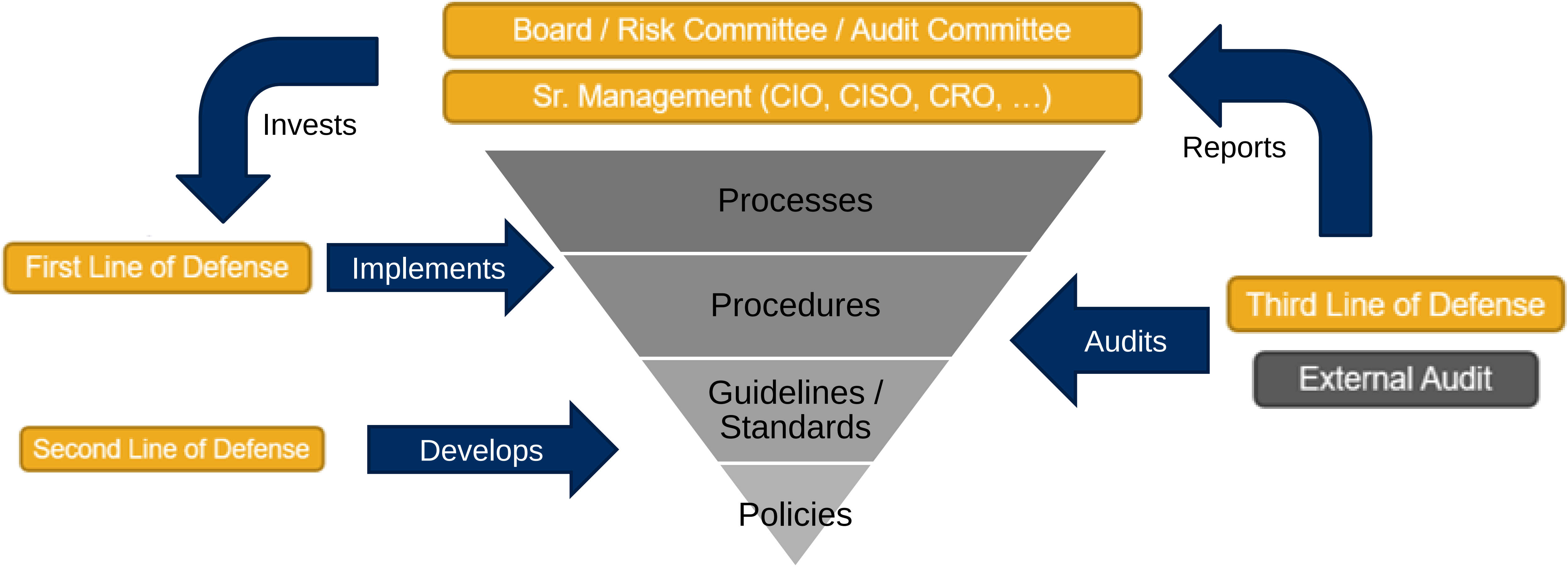
Internal Audit

External Audit

Regulators

*Adapted from ECIIA/FERMA Guidance on 8th EU Company Law Directive, article 41

Policies, Procedures, & Processes



Board / Risk Committee / Audit Committee

Sr. Management (CIO, CISO, CRO, …)

Invests

Reports

Processes

Procedures

Guidelines / Standards

Policies

First Line of Defense

Implements

Second Line of Defense

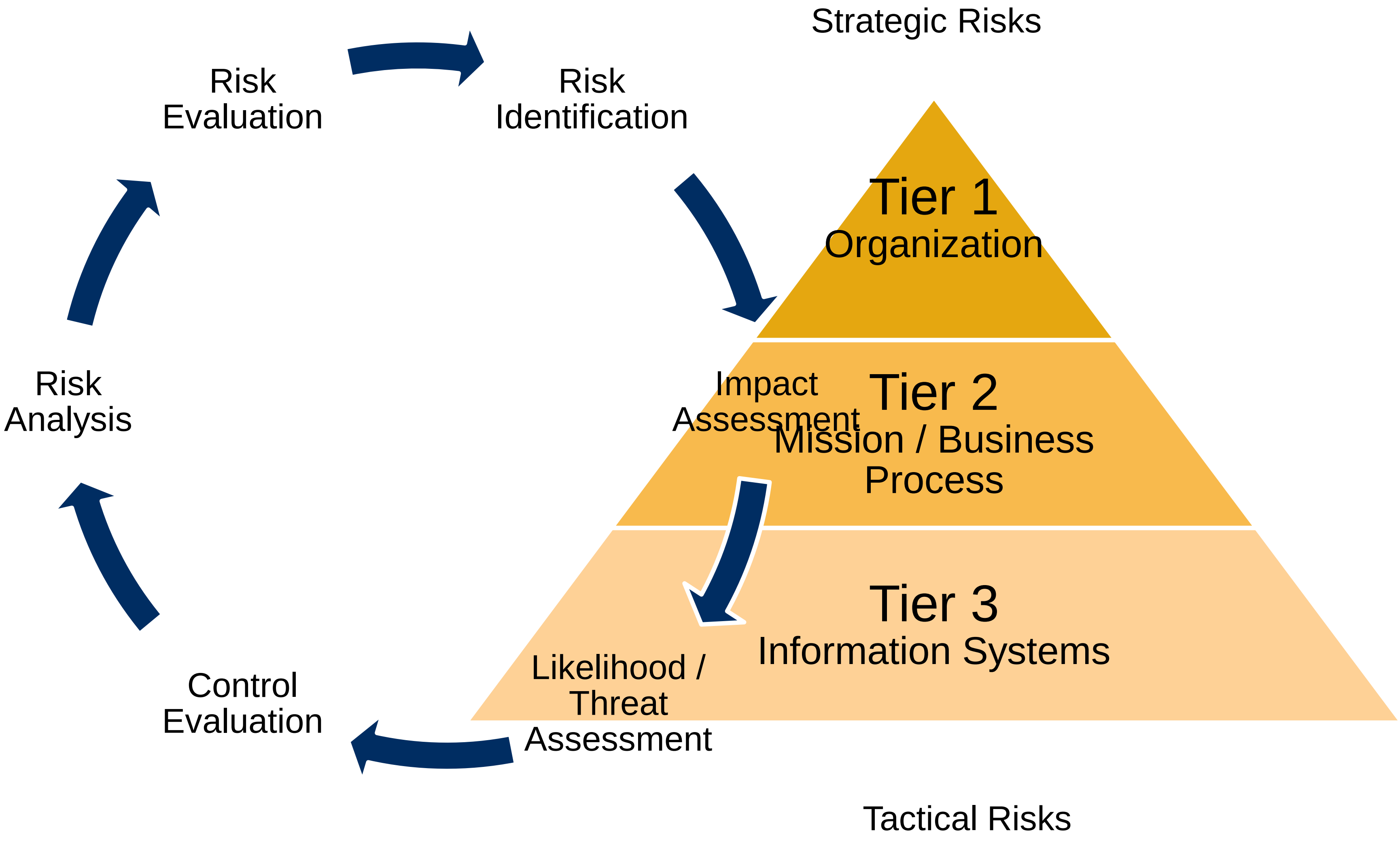
Develops

Third Line of Defense

Audits

External Audit

Risk Assessment



* Adapted from NIST SP 800-30 “Guide for Conducting Risk Assessments”

Continuous Monitoring

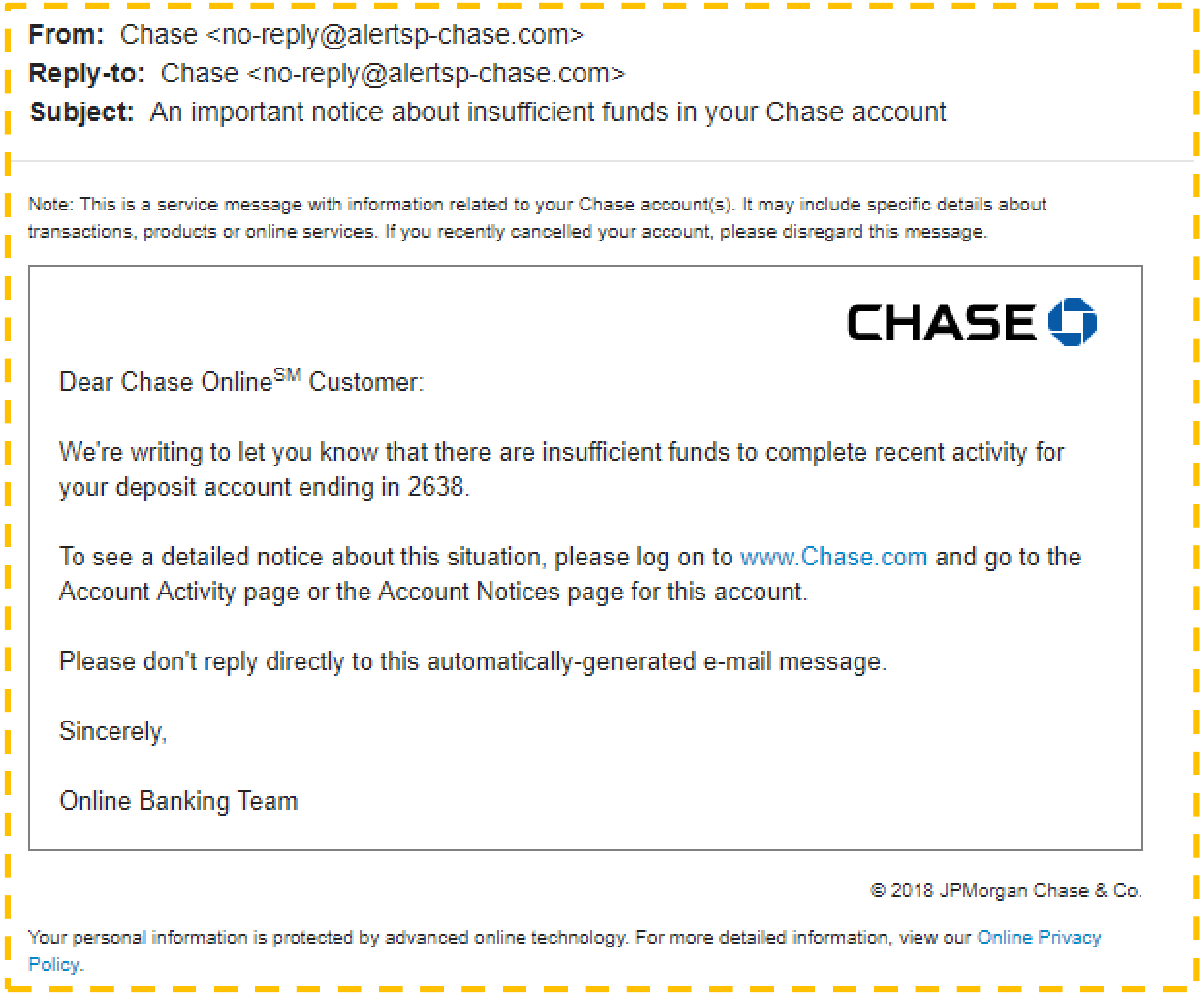
Key Steps for Continuous Monitoring:

1. Identify and define criteria for monitoring
2. Specify frequency, ownership, and deliverable
3. Integrate with risk management strategy

- Examples:
  - Second Line - Access reviews, alerts; Program Metrics
  - Third Line - Auditing

Top Risk #1: Phishing

Importance of Security Awareness



From: Chase <no-reply@alertsp-chase.com>
Reply-to: Chase <no-reply@alertsp-chase.com>
Subject: An important notice about insufficient funds in your Chase account

Note: This is a service message with information related to your Chase account(s). It may include specific details about transactions, products or online services. If you recently cancelled your account, please disregard this message.

CHASE

Dear Chase Online^{SM} Customer:

We're writing to let you know that there are insufficient funds to complete recent activity for your deposit account ending in 2638.

To see a detailed notice about this situation, please log on to www.Chase.com and go to the Account Activity page or the Account Notices page for this account.

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,

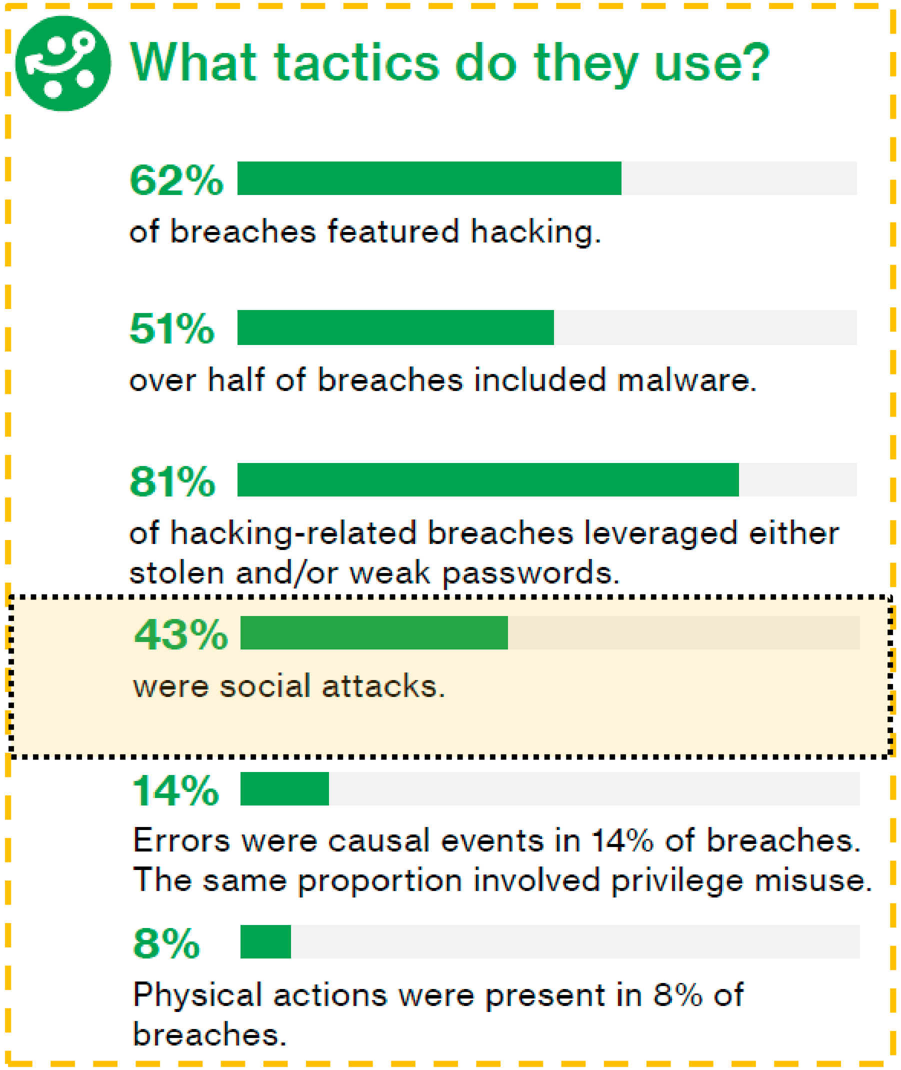
Online Banking Team

© 2018 JPMorgan Chase & Co.

Your personal information is protected by advanced online technology. For more detailed information, view our Online Privacy Policy.

Importance of Security Awareness

The 2017 Verizon Data Breach report states that over 43% of the data breaches reported originated from social actions (social engineering) and, of those, over 90% were via phishing.



What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

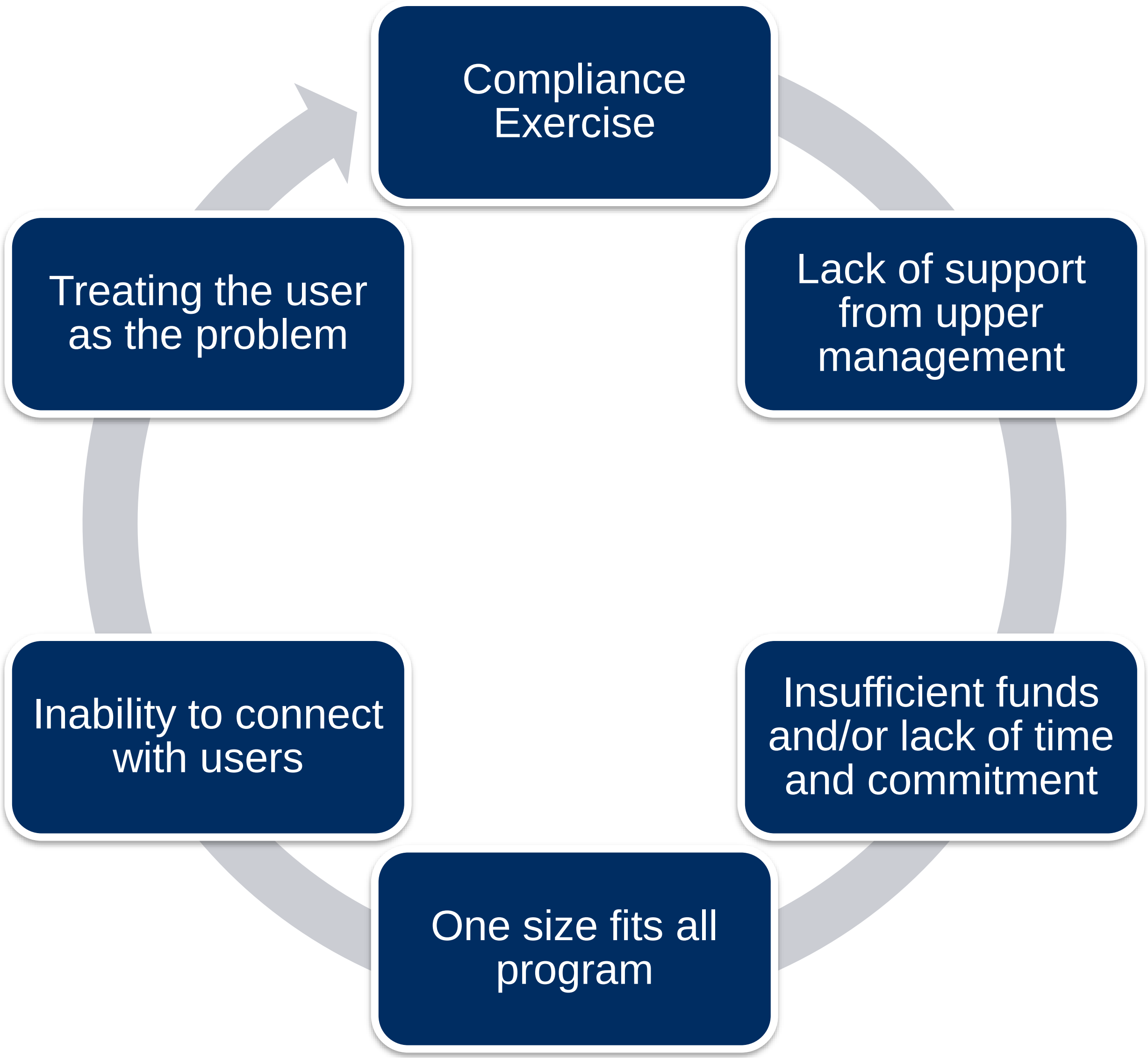
14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

Source: Verizon 2017 Data Breach Report

Historical Security Awareness

Traditional limitations to security awareness



Compliance Exercise

Lack of support from upper management

Insufficient funds and/or lack of time and commitment

One size fits all program

Inability to connect with users

Treating the user as the problem

Security Awareness Best Practices

Change Agent

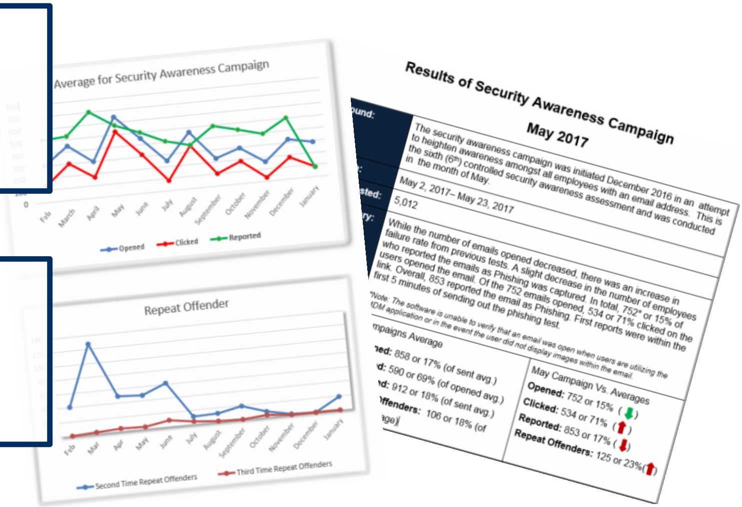
- Incorporate themes, a tagline, a mascot, etc. that’s simple & memorable to create an employee connection

NIKE

"Just do it"

Sufficient Testing

- Perform ongoing simulated phishing tests and periodically perform in-person and phone social engineering.



Results of Security Awareness Campaign

May 2017

ound: The security awareness campaign was initiated December 2016 in an attempt to heighten awareness amongst all employees with an email address. This is the sixth (6th) controlled security awareness assessment and was conducted in the month of May.

: May 2, 2017– May 23, 2017

sted: 5,012

ry: While the number of emails opened decreased, there was an increase in failure rate from previous tests. A slight decrease in the number of employees who reported the emails as Phishing was captured. In total, 752* or 15% of users opened the email. Of the 752 emails opened, 534 or 71% clicked on the link. Overall, 853 reported the email as Phishing. First reports were within the first 5 minutes of sending out the phishing test.

Note: The software is unable to verify that an email was open when users are utilizing the IDM application or in the event the user did not display images within the email.

mpaigns Average
ned: 858 or 17% (of sent avg.)
d: 590 or 69% (of opened avg.)
d: 912 or 18% (of sent avg.)
ffenders: 106 or 18% (of
age)

May Campaign Vs. Averages
Opened: 752 or 15% (⬇)
Clicked: 534 or 71% (⬆)
Reported: 853 or 17% (⬇)
Repeat Offenders: 125 or 23%(⬆)

Tailored Training

- Perform trainings based on an employee’s risk level. Use gamification strategies and consider generational learning preferences

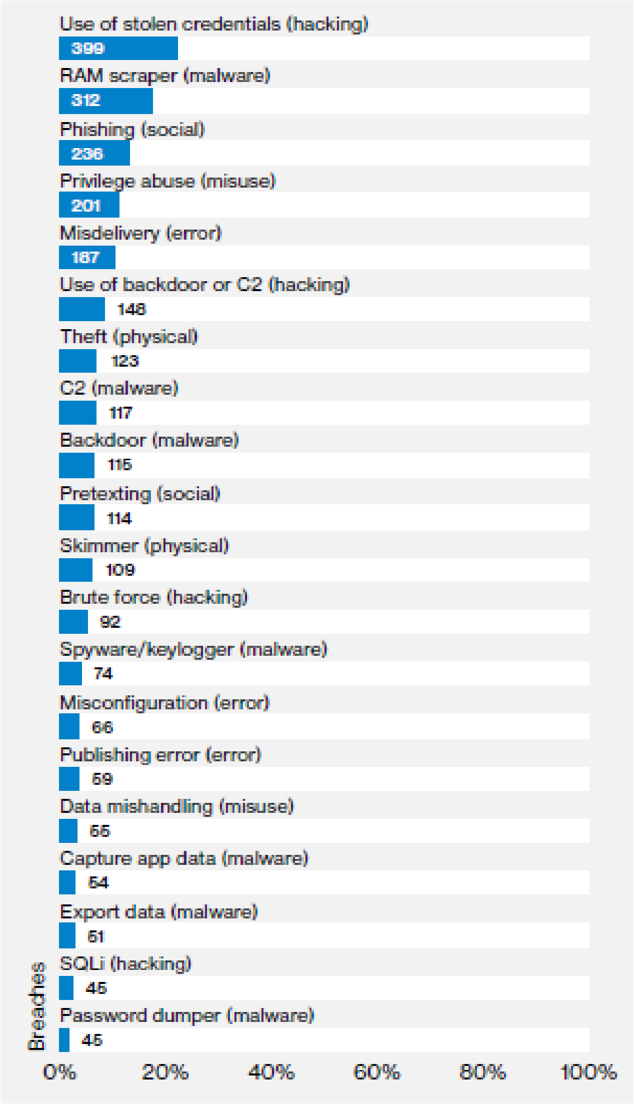
Multiple Mediums

- Email, social media, videos, and in-person resources.

Top Risk #2: User Access & Authentication

Top Actions of Breaches

22% of confirmed breaches in 2018 used stolen credentials.



**Source: Verizon 2018 Data Breach Report*

Common Access Issues

1. Weak password requirements / easily guessable passwords

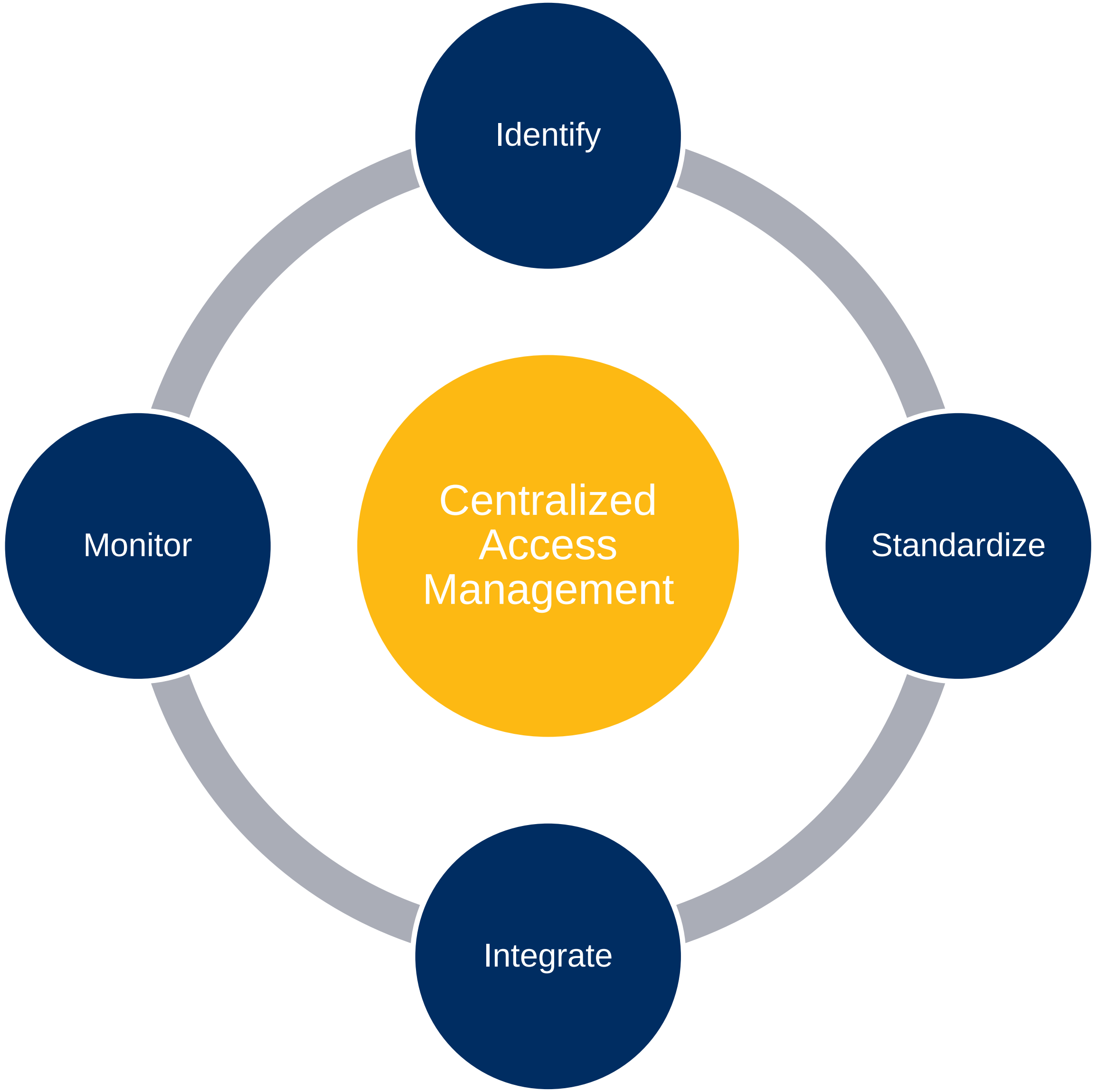
2. Account privileges are not reviewed

3. Unmanaged vendor/contractor accounts

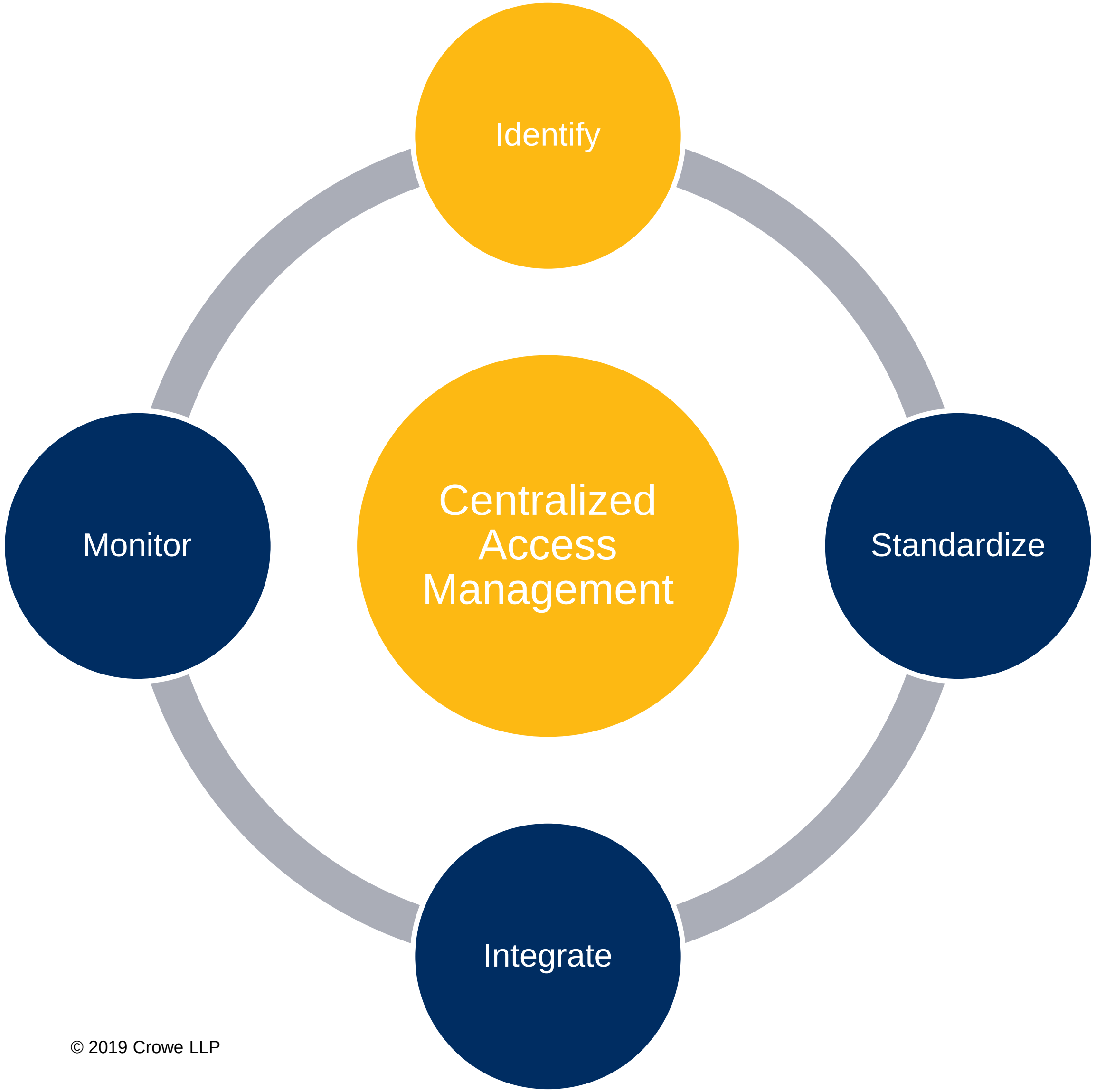
4. Multi-factor authentication is not used for remote system access

5. Default passwords are not changed

Building an Access Management Program



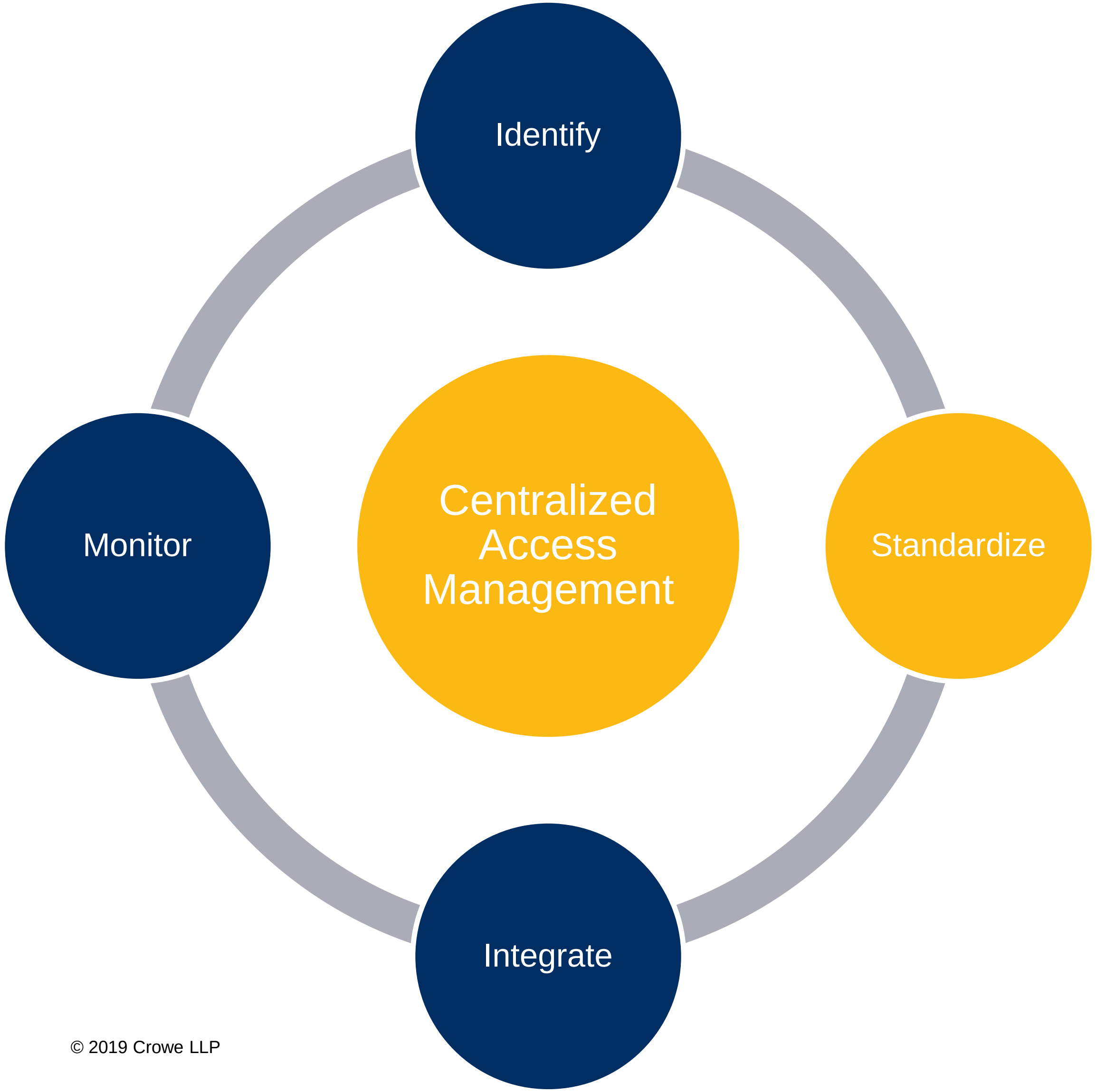
Building an Access Management Program



Determine how system access is provided and what information is provided

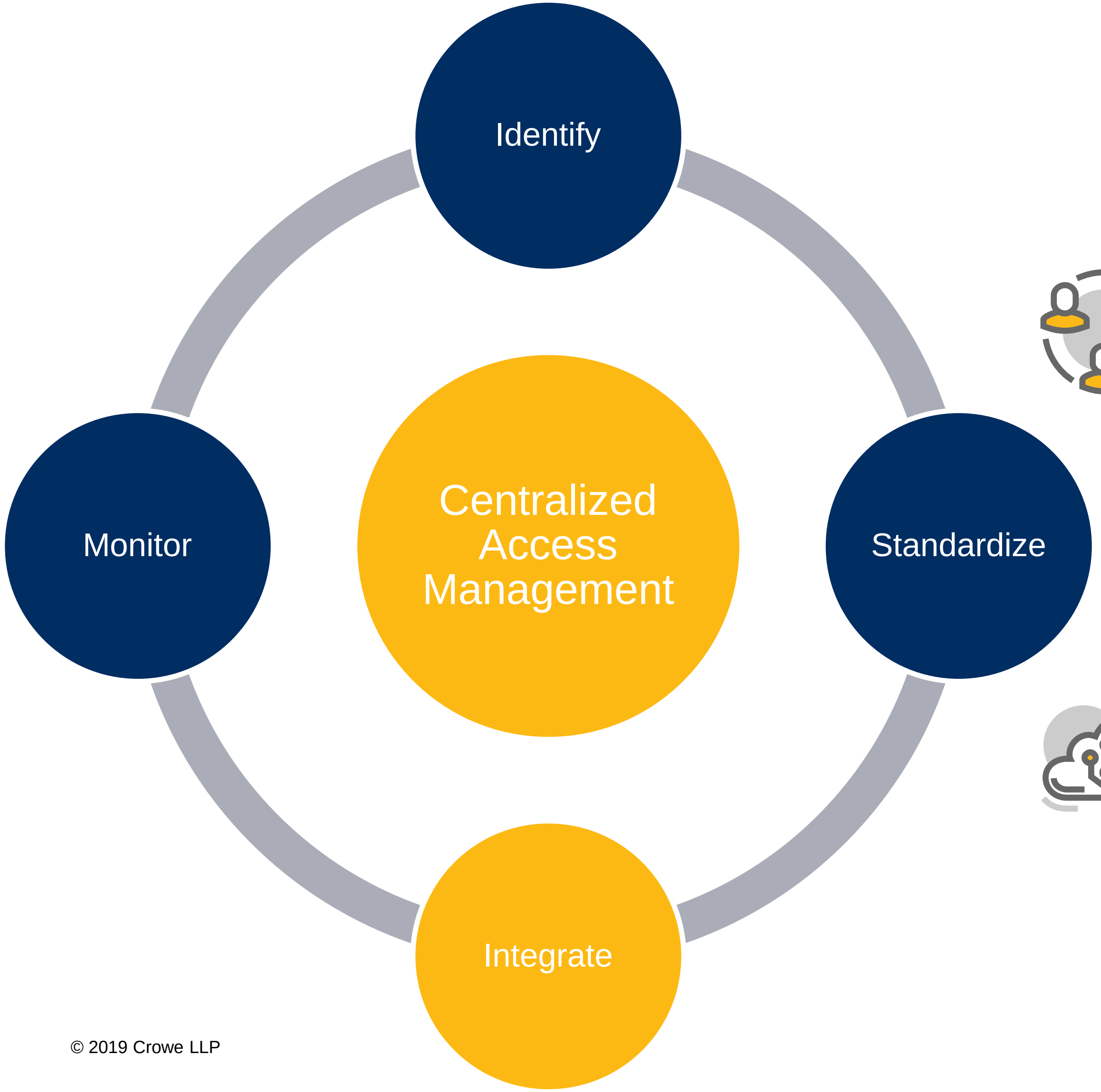
“You can’t secure what you can’t see”

Building an Access Management Program



National Institute of Standards and Technology

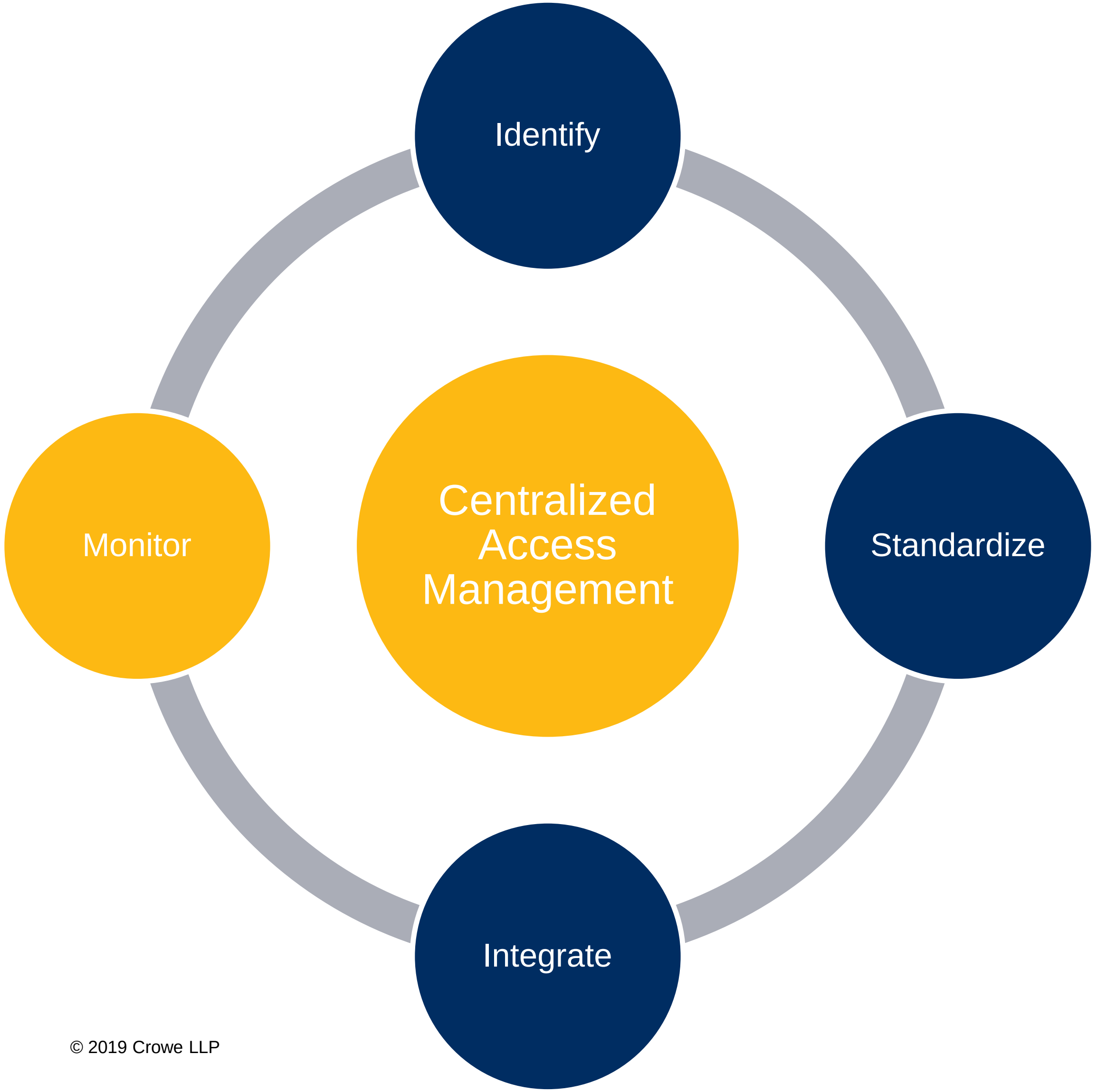
Building an Access Management Program



Have a *single* team that manages access

Use technologies like SAML, SSO, etc. to *simplify* management

Building an Access Management Program



Access Reviews:

✓ Inactive accounts & terminated employees

✓ Account privileges

✓ Account activity

Authentication Best Practices

- “Risk-Based” Authentication
  - MFA for remote access
  - Complex administrator passwords
- Automatic account expiration
- “Tap-and-go” authentication for clinicians
- Password dictionaries

Top Risk #3: Mobile & Biomedical Devices

Medical device security is lacking

Only 9%

of manufacturers say they test medical devices at least annually.

Only 51%

of device makers say they follow guidance from the FDA to mitigate or reduce inherent security risks in medical devices.

Unsurprisingly, 67%

of device makers believe it is likely there will be an attack on one of the devices they've built within the next 12 months. —*Ponemon 2017*

Sources:
Ponemon Institute: Medical Device Security: An Industry Under Attack and Underprepared to Defend, May 2017

Balancing Benefits and Risks of Medical Devices

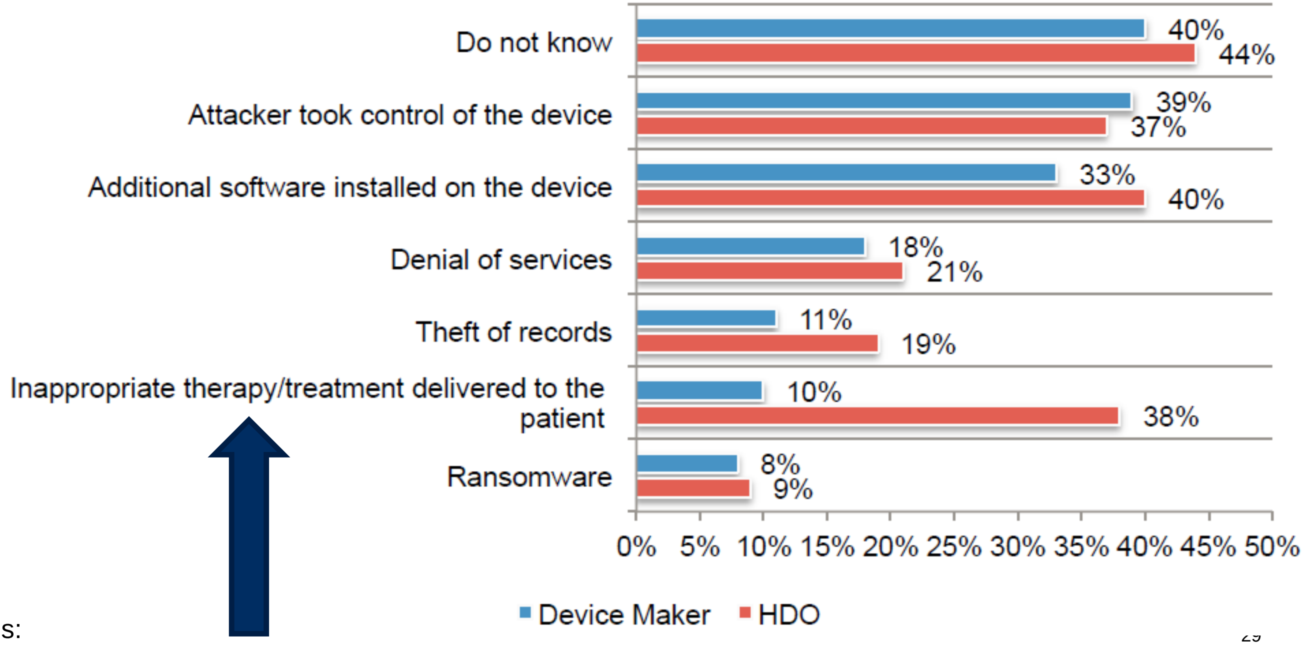
Medical Device Benefits

Today’s medical devices help reduce healthcare costs while allowing people to better manage their conditions. *The use of remote monitoring to improve the health of people with chronic diseases is estimated to save as much as $1.1 trillion per year by 2025.*

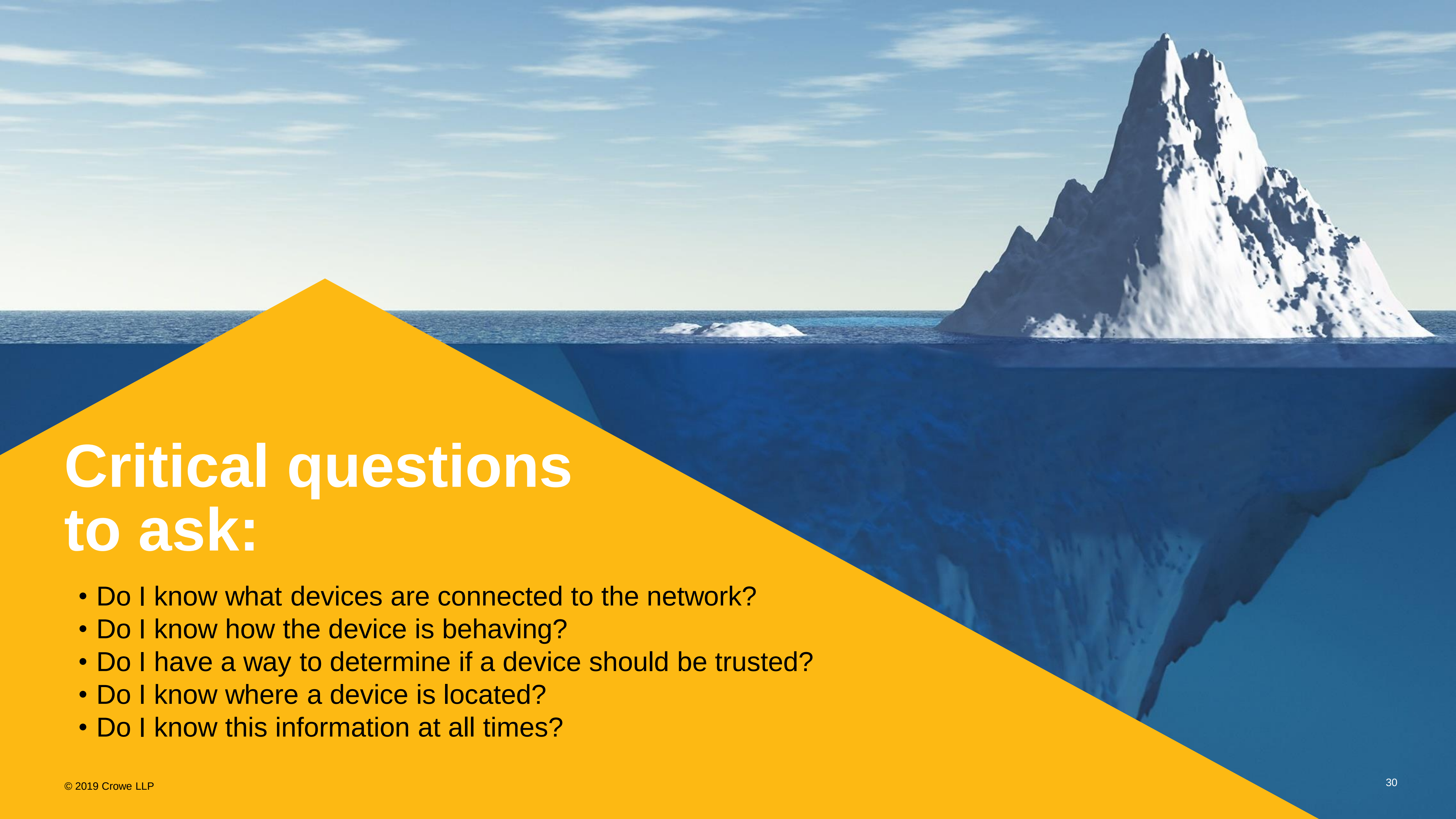
Medical Device Risks

But these devices aren’t without risks to patient safety and continuity of care.

- *Ransomware attacks*
- *Vulnerabilities in implantable devices*
- *Tele-care or tele-health interruptions*
- *Vulnerabilities in medical devices such as imaging, diagnostic, etc.*



Sources:
Ponemon Institute: Medical Device Security: An Industry Under Attack and Underprepared to Defend, May 2017



Critical questions to ask:

- Do I know what devices are connected to the network?
- Do I know how the device is behaving?
- Do I have a way to determine if a device should be trusted?
- Do I know where a device is located?
- Do I know this information at all times?

Device Inventory

Risk Assessment Process

Configuration Standards

Cross-Functional Oversight Committee

Biomedical Device Management Program

Top Risk #4: Business Continuity Management

How prepared are you?

- In 2017, approximately **47.5%** of IT employees and C-level executives believe they are just "somewhat prepared" to recover their IT and related assets in the event of a disaster or other incident

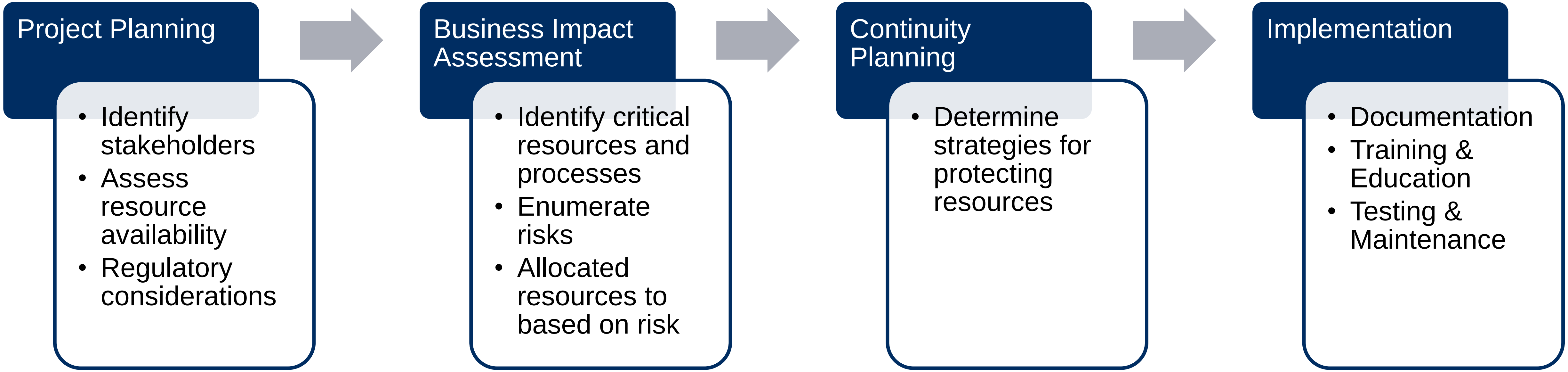
- From the same survey, **less than half** of firms in the same survey had tested their DR plan in 2017

BCM – Common Pitfalls

- Generally, organization’s excel at continuity of care
- As it relates to IT, common issues include:
  - Integrating business stakeholders
  - Insufficient documentation
  - Testing and Training

- As a result:
  - IT cannot recover systems to meet operational requirements
  - High/unnecessary costs associated with recovery technologies
  - Lack of familiarity with response/recovery procedures

Business Continuity Planning Process



Project Planning

- Identify stakeholders
- Assess resource availability
- Regulatory considerations

Business Impact Assessment

- Identify critical resources and processes
- Enumerate risks
- Allocated resources to based on risk

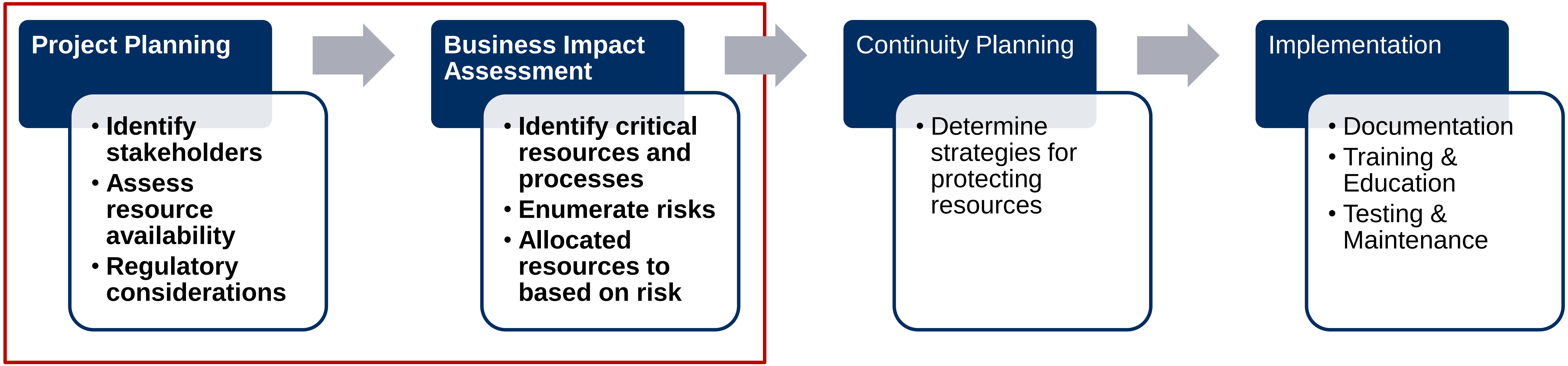
Continuity Planning

- Determine strategies for protecting resources

Implementation

- Documentation
- Training & Education
- Testing & Maintenance

Integrating Business Stakeholders



Project Planning

- **Identify stakeholders**
- **Assess resource availability**
- **Regulatory considerations**

Business Impact Assessment

- **Identify critical resources and processes**
- **Enumerate risks**
- **Allocated resources to based on risk**

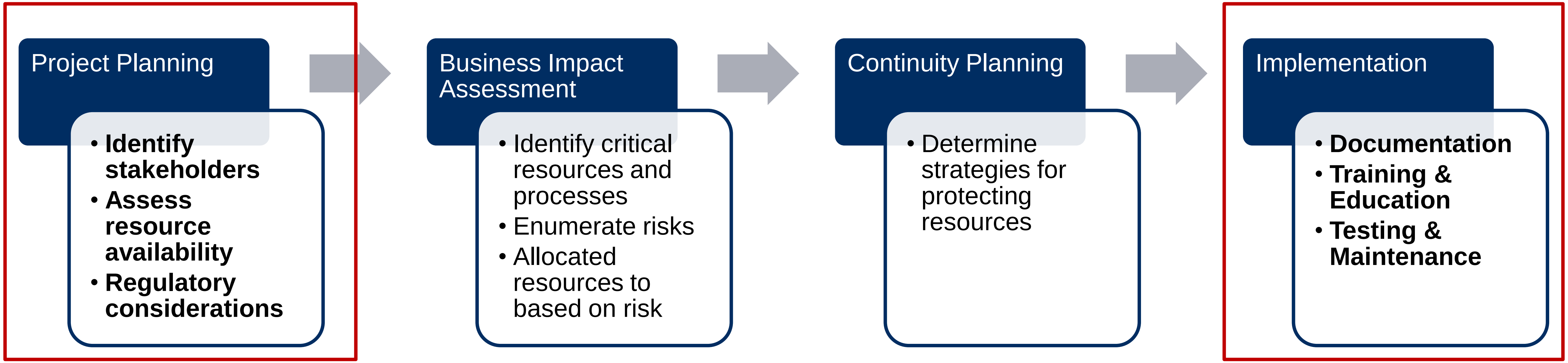
Continuity Planning

- Determine strategies for protecting resources

Implementation

- Documentation
- Training & Education
- Testing & Maintenance

Documentation, Testing, and Training



Project Planning

- **Identify stakeholders**
- **Assess resource availability**
- **Regulatory considerations**

Business Impact Assessment

- Identify critical resources and processes
- Enumerate risks
- Allocated resources to based on risk

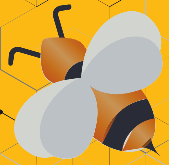
Continuity Planning

- Determine strategies for protecting resources

Implementation

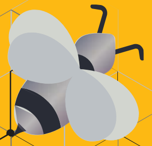
- **Documentation**
- **Training & Education**
- **Testing & Maintenance**

Questions



Introducing Healthcare’s Trusted Community:

The Crowe Hive Network



Being successful in your role today looks different than it did even a few years ago. **Engage with a network of those who have been there before you:**

- Ask and answer community questions
- Seek validation and gain support through crowdsourcing
- Connect with peers and Crowe specialists
- Earn rewards for your engagement and shop the Hive store

Simplify your busy workday. Register today to continue the Healthcare Summit conversations: **crowehive.com.**

Thank you

James Kernen, CISA, CISSP, CFE, CMA
Senior Manager
+1 818 325 8453
James.Kernen@crowehrc.com

Alex Hiznay, Associate CISSP
Senior Consultant
+1 646 356 4481
Alexander.Hiznay@crowe.com