Beyond Cybersecurity: Protecting Your Digital Business

Discussion Document
June 9th, 2016

CONFIDENTIAL AND PROPRIETARY
Any use of this material without specific permission of McKinsey & Company is strictly prohibited

Overview

- Current cybersecurity approaches getting in the way of companies’ efforts to capture value from digitization
- Better model for protecting critical information requires much tighter integration with rest of the business, but most companies aren’t making sufficient progress
- Getting beyond cybersecurity to digital resilience is a cross-functional change – making progress requires:
  - Designing change program to drive business engagement,
  - Creating a culture of resiliency across IT
  - Professionalizing cybersecurity capabilities

Rapid digitization raises the stakes for issues of trust and data protection in health care

<table>
<thead>
<tr>
<th>Increased digitization of care delivery</th>
<th>Introduce new security risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vastly expanded technology environment introducing more surfaces and opportunities for attack</td>
<td></td>
</tr>
<tr>
<td>Increased interconnectivity with external systems (e.g., exchanges, vendors)</td>
<td></td>
</tr>
<tr>
<td>Increased exposure of individual assets across an organization (e.g., PHI)</td>
<td></td>
</tr>
<tr>
<td>Increasing cost of data breaches (e.g., cost of breach, HIPAA fines from $100-$25K per record)</td>
<td></td>
</tr>
<tr>
<td>Emerging technologies becoming embedded in “everyday” operations and devices outside traditional IT function boundaries</td>
<td></td>
</tr>
<tr>
<td>Additional customer demands for security and proof of security standards, from members and employee groups</td>
<td></td>
</tr>
</tbody>
</table>
Participants in the health ecosystem exchanging sensitive data and interconnecting networks

SOURCE: McKinsey analysis

Cybersecurity spend in healthcare continues to increase

Cybersecurity expenditure as a percent of total IT expenditure, Percent

Current Spend

<table>
<thead>
<tr>
<th>Hospital network</th>
<th>Hospital network</th>
<th>Hospital network</th>
<th>Health payer</th>
<th>Pharma</th>
<th>Pharma</th>
<th>Pharma</th>
<th>Pharma</th>
<th>Pharma</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>4.1</td>
<td>3.2</td>
<td>4.3</td>
<td>2.8</td>
<td>4.0</td>
<td>5.6</td>
<td>2.0</td>
<td></td>
</tr>
</tbody>
</table>

Expected change in next 3 yrs

- Decrease slightly
- Increase significantly
- Increase materially
- Increase substantially
- Decrease
- Flat to decrease
- Increase
- Increase as uplift program concludes
- Decrease

SOURCE: HC CISO Survey

Traditional cybersecurity models already putting 'sand in the gears' for digital enterprises

Traditional cybersecurity models drive...

- Slower technology innovation
- Reduced resources for value-creating IT
- Slower implementation of technology innovations
- Increased time and effort to contract for goods and services
- Increase in length of sales cycle
- Increase in length of total IT activity driven by security requirements
- 60% high tech, executives who say productivity impacted
- 18 months delay in using public cloud infrastructure services as a result of cybersecurity considerations
- 2x increase in length of sales cycle over past ten years as a result of cybersecurity considerations, according to entrepreneurial software CEOs

Risks

1. Prioritize information assets and related risks
2. Use prioritized risk matrix to drive decisions about
   security investments and policies

Hallmarks of digital resilience – most companies not making
sufficient progress

Critical resiliency levers

1. Prioritize information assets and related risks in a way that
   helps engage business leaders
2. Endfront-line personnel – helping them understand value
   of information assets
3. Integrate cyber-resilience into enterprise risk management
   and governance processes
4. Integrated incident response across business functions,
   anchored by realistic testing
5. Driving deep integration of security into the technology
   environment to drive security
6. Provide differentiated protection for most important
   assets
7. Deploy active defenses to be proactive in uncovering attacks
   early

Percentage of IT Executives Indicating

<table>
<thead>
<tr>
<th>Critical resiliency lever</th>
<th>Percent of IT Executives Indicating</th>
<th>Average performance, 1-4 scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>74%</td>
<td>1.9</td>
</tr>
<tr>
<td>2</td>
<td>60%</td>
<td>2.2</td>
</tr>
<tr>
<td>3</td>
<td>55%</td>
<td>2.6</td>
</tr>
<tr>
<td>4</td>
<td>65%</td>
<td>2.6</td>
</tr>
<tr>
<td>5</td>
<td>86%</td>
<td>2.6</td>
</tr>
<tr>
<td>6</td>
<td>74%</td>
<td>2.7</td>
</tr>
<tr>
<td>7</td>
<td>75%</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Use prioritized risk matrix to drive decisions about
security investments and policies

Finding risk (likelihood against impact helps focus investment)

Risk:

A. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)
B. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)
C. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)
D. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)
E. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)
F. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)

Likelihood:

Low Medium High

E. Theft of customer PII data
   - Phishing associated login credentials
   - Mobile device owner solution
   - Customer PII data in malicious code
   - Customer PII data in malicious code (e.g., malicious code by
     vendor)

McKinsey & Company
Example prototype for customer security program

<table>
<thead>
<tr>
<th>Your personal risk factors</th>
<th>Account control options</th>
<th>Account security</th>
</tr>
</thead>
<tbody>
<tr>
<td>High average monthly account balance</td>
<td>☑ Complex password required</td>
<td>Maximum</td>
</tr>
<tr>
<td>High monthly average transaction volume</td>
<td>☑ Password change required every 90 days</td>
<td>Minimum Recommended</td>
</tr>
<tr>
<td>More than ten international trips per year</td>
<td>☑ SMS-based authentication</td>
<td>Minimum allowed</td>
</tr>
<tr>
<td>Accessed account from more than 5 different devices in the past year</td>
<td>☑ Graduated authentication for payment transactions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☑ SMS-based notification for all transactions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☑ Device authentication</td>
<td></td>
</tr>
</tbody>
</table>

More efficient and effective to build security into modernized technology architecture

- Move to near pervasive client virtualization to reduce desktop, laptop and mobile devices as a source of vulnerability
- Use software-defined networking to compartmentalize the network, limiting lateral movement and reducing operational complexity
- Build security into the application, creating developer capabilities (e.g. skills, tools, platforms) from the start
- Stop using email as a document management and workflow tool
- Accelerate migration to private cloud to get benefits of improved transparency and patch management

Structural and organizational challenges make it hard to achieve digital resilience

Issues
1. Digital resilience requires change across the organization – in business processes, user behavior, business applications and technology infrastructure
2. Business leaders find it hard to engage on cybersecurity – language is arcane, scare stories are common and useful metrics are scarce
3. IT managers traditionally focused on delivering functionality quickly and minimizing cost – not resiliency
4. Cybersecurity managers lack skills to engage business effectively

Implications
- Hard to get input and alignment from business leaders on:
  - Most important business risks and information assets
  - How to segment and influence users
  - How to change business processes to improve resiliency
- Security program treated as a separate, incremental stream of work from other IT priorities
- Over-reliance on technical controls and policy restrictions that increase cost and complexity
- Security program seen as “more of the same” – increasing organizational resistance and slowing change
**Example: re-launching cybersecurity program for health care provider**

1. Define the decision context:
   - Understand the health care provider’s unique challenges.

2. Define the overarching cyber framework:
   - Develop a strategy tailored to the provider’s needs.

3. Onboard stakeholders and align on governing concerns:
   - Ensure all parties are aligned on the program’s goals.

4. Assess current risk posture (McKinsey DRS):
   - Evaluate the current state of the provider’s cybersecurity.

5. Prioritize risks and identify of Crown jewels:
   - Focus on critical areas that require immediate attention.

6. Define different business units’ (BU) context:
   - Tailor strategies to the specific needs of each business unit.

7. Dedicated track for Edge devices given provider context:
   - Address specific security requirements for边缘 devices.

8. Executive war games to test response preparedness:
   - Enhance readiness through simulation exercises.

9. Develop dashboards to run programs effectively:
   - Use data-driven insights to drive program outcomes.

10. Run war games and check progress quarterly:
    - Regularly assess and adjust the program to ensure alignment.

---

**Example Output**

Provides granular insight into performance across different businesses or divisions:

<table>
<thead>
<tr>
<th>Area</th>
<th>BU 1</th>
<th>BU 2</th>
<th>BU 3</th>
<th>BU 4</th>
<th>BU 5</th>
<th>BU 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>2.5</td>
<td>2.7</td>
<td>1.5</td>
<td>2.0</td>
<td>1.7</td>
<td>0.5</td>
</tr>
<tr>
<td>Business process adequacy</td>
<td>2.0</td>
<td>2.0</td>
<td>2.5</td>
<td>1.5</td>
<td>1.8</td>
<td>1.2</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>1.5</td>
<td>1.5</td>
<td>1.6</td>
<td>1.6</td>
<td>1.0</td>
<td>0.8</td>
</tr>
<tr>
<td>Compliance and audit</td>
<td>3.0</td>
<td>3.0</td>
<td>2.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Cyber intelligence and vulnerability</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Gap analysis at information asset and system levels guides targeted remediation investments**

1. Identify information assets and business risks:
   - Understand the critical assets and potential threats.

2. Enlist front-line personnel to help them understand the value of information assets:
   - Engage all levels of the organization in the program.

3. Integrate cyber-resilience into enterprise-wide management and governance processes:
   - Embed cybersecurity into all aspects of the organization.

4. Develop deep integration of security into the technology environment to drive scalability:
   - Ensure security is a core component of all technological solutions.

5. Provide differentiated protection for most important assets:
   - Implement tailored security measures for critical assets.

6. Deploy active defenses to respond to emerging attacks in real time:
   - Stay ahead of potential threats.

---

**McKinsey Proprietary tools to support**

- Organize around program tracks aligned with outcomes.
- Deep-dives into specific large initiatives e.g., NW Segment.
- Align on desired outcomes, maturity level and residual risk.
- Develop dashboards to run programs effectively.
- Run war games and check progress quarterly.

**McKinsey & Company**
Services you could leverage: CyberFit, the healthcare cybersecurity services provider Utility

What is the healthcare cyber utility?

A not-for-profit, shared “utility” that is:

- Owned by members, governed by members for the benefit of members
- Enabled by collaborative efforts of member healthcare organizations
- Structured to provide access to best-in-class cyber security services to healthcare organizations of all types and sizes

Why should it exist?

The healthcare cyber utility is in a unique position to:

- Create member-supported healthcare-specific capabilities that do not and could not exist in the marketplace without the utility
- Help “immunize” the entire industry—with larger organizations making critical cyber security services available to smaller healthcare organizations, which otherwise would not have access to these critical services
- Leverage scale to boost efficacy of solutions and benefits, and to increase ability to influence stakeholders
- Address the changing regulatory landscape better than a single organization
- Establish standards or control framework that can provide adopting organizations better defensibility against legal issues
- Enable members to free up scarce resources from commodity tasks to focus on high value add activities

What is the healthcare cyber utility?

Why should it exist?

- Create member-supported healthcare-specific capabilities that do not and could not exist in the marketplace without the utility
- Help “immunize” the entire industry—with larger organizations making critical cyber security services available to smaller healthcare organizations, which otherwise would not have access to these critical services
- Leverage scale to boost efficacy of solutions and benefits, and to increase ability to influence stakeholders
- Address the changing regulatory landscape better than a single organization
- Establish standards or control framework that can provide adopting organizations better defensibility against legal issues
- Enable members to free up scarce resources from commodity tasks to focus on high value add activities

Services CyberFit will offer

<table>
<thead>
<tr>
<th>Description of MVP service</th>
<th>MVP Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy &amp; Regulatory updates</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Online assessment on several dimensions of digital resiliency</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Service to focus on events in North America and select countries</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Legal analysis, and updates beyond standard published reports</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Organizational benchmarks</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Online assessment that extends beyond standard published reports</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Benchmarks and comparisons with healthcare/other industry peers</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Standard reports with assessment history and maturity trail</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>3rd-party risk assessments</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Library of assessments based on common assessment criteria applied to assessments from various contributors</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Standard risk assessments for industry best vendors, and custom assessments based on subscriber specific criteria</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Vulnerability &amp; pen testing</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Penetration testing/ Vulnerability scanning based on Utility security standards</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Best-in-class recommendation based on test and analysis and roadmap to achieve better resiliency</td>
<td>Q3, 2016</td>
</tr>
<tr>
<td>Shared SOC</td>
<td>Q4, 2016</td>
</tr>
<tr>
<td>Vendor provided shared SOC, potentially at a low-cost location</td>
<td>Q4, 2016</td>
</tr>
</tbody>
</table>

Questions?

James_Kaplan@mckinsey.com
Venky_anant@mckinsey.com