

Beyond Cybersecurity: Protecting Your Digital Business

Discussion Document
June 5th, 2016

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

McKinsey&Company







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

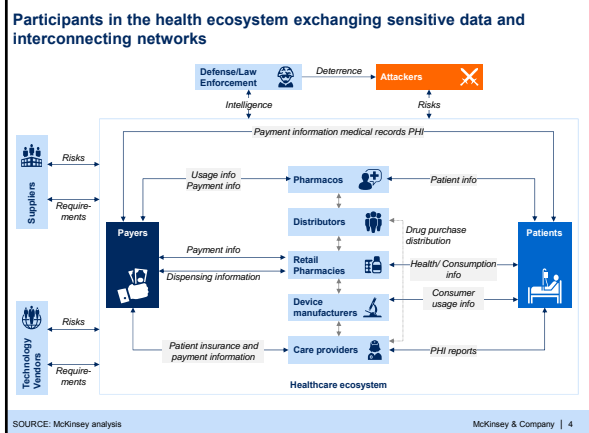
McKinsey & Company | 2

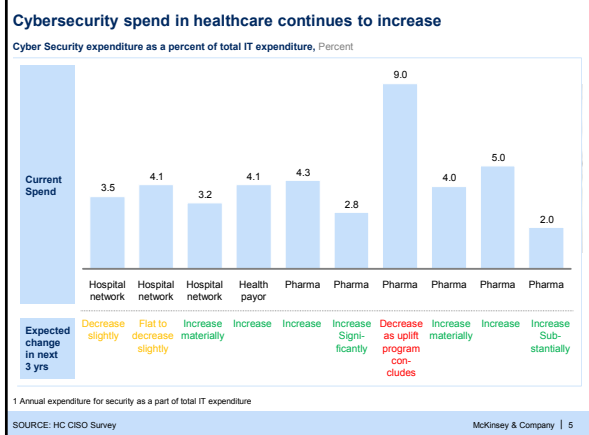
Rapid digitization raises the stakes for issues of trust and data protection in health care

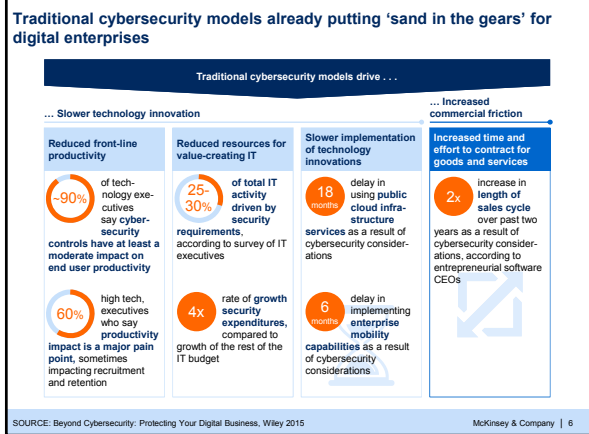
Increased digitization of care delivery introduce new security risks

 <p>Vastly expanded technology environment introducing more surfaces and opportunities for attack</p>	 <p>Increased interconnectivity with external systems (e.g., exchanges, vendors)</p>	 <p>Increased exposure of individual assets across an organization (e.g., EHRs)</p>
 <p>Increasing cost of data breaches (e.g., cost of breach, HIPAA fines from \$100-\$2K per record)</p>	 <p>Emerging technologies becoming embedded in "every-day" operations and devices outside traditional IT function boundaries</p>	 <p>Additional customer demands for security and proof of security standards, from members and employee groups</p>

McKinsey & Company | 3







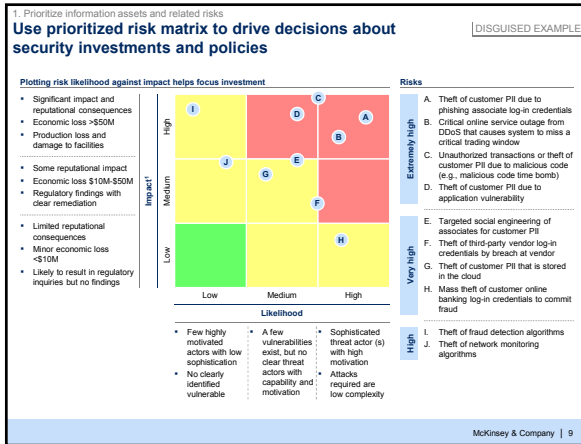
Existing models are increasingly less tenable as threats scale

High	<p>Digital resilience 2014-2020</p> <ul style="list-style-type: none">• Clear alignment with business on what to protect and how• Cyber-security risks implications integrated into business decision-making• "Security inside" for most elements of IT environment• Increased business integration enables tighter controls, with less friction
Low	<p>Cyber-security as a control function 2007-2013</p> <ul style="list-style-type: none">• Increased governance authority for cyber-security• End user environment "locked down," but users frustrated with reduced flexibility• Architectural reviews reduce risks, but slow introduction of new capabilities
	<p>Cyber-security not a priority Pre-2007</p> <ul style="list-style-type: none">• Cyber-security under-funded• Little insight into business risks or technology vulnerabilities• Protections focused on the perimeter• Few consequences for violating policies• Insecure application code and infrastructure configurations common

Most institutions are operating in this model

- Places the responsibility for security mostly on the security team
- Backward looking – puts protections in place against yesterday's attacks
- Dependent on manual interventions – not scalable
- Dependent on checks and double checks
- Increasing tension between security and innovation and flexibility

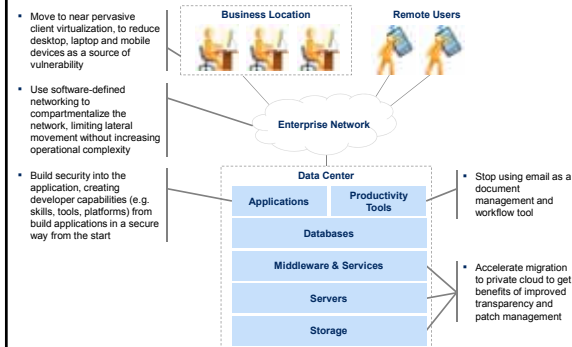
McKinsey & Company | 7

[illegible]

Example prototype for customer security program

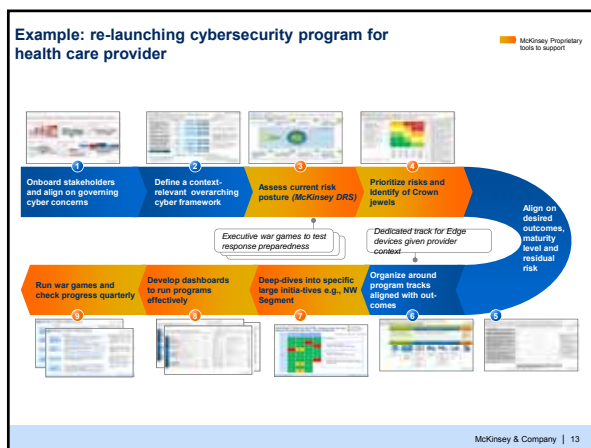
Your personal risk factors	Account control options	Account security
<input checked="" type="checkbox"/> High average monthly account balance <input checked="" type="checkbox"/> High monthly average transaction volume <input checked="" type="checkbox"/> More than ten international trips per year <input checked="" type="checkbox"/> Accessed account from more than 3 different devices in the past year	<input type="checkbox"/> Complex password required <input type="checkbox"/> Password change required every 90 days <input checked="" type="checkbox"/> SMS-based authentication <input checked="" type="checkbox"/> Graduated authentication for payment transactions <input checked="" type="checkbox"/> SMS-based notification for all transactions <input type="checkbox"/> Device authentication	<div> <div>Maximum</div> <div>Minimum Recommended</div> <div>Minimum allowed</div> </div>

More efficient and effective to build security into modernized technology architecture



Structural and organizational challenges make it hard to achieve digital resilience

Issues	Implications
<ol style="list-style-type: none"> Digital resilience requires change across the organization – in business processes, user behavior, business applications and technology infrastructure Business leaders find it hard to engage on cybersecurity – language is arcane; scare stories are common and useful metrics are scarce IT managers traditionally focused on delivering functionality quickly and minimizing cost – not resiliency Cybersecurity managers lack skills to engage business effectively 	<ul style="list-style-type: none"> Hard to get input and alignment from business leaders on <ul style="list-style-type: none"> 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



Provides granular insight into performance across different businesses or divisions

EXAMPLE OUTPUT

Legend: ■ ≥3.0 (High) ■ 2.0-2.9 ■ <2.0 (Low)

		BU 1	BU 2	BU 3	BU 4	BU 5	BU 6
1	Prioritize information assets and business risks in a way that helps engage business leaders	2.2	3.4	2.4	1.6	1.3	2.3
	Asset and risk prioritization	1.3	4.0	2.0	3.0	2.5	2.0
	Risk appetite and thresholds	2.0	3.0	3.0	3.3	1.7	3.3
2	Enlist front-line personnel – helping them understand value of information assets	2.1	2.7	2.1	1.6	1.9	1.7
	Awareness, training and risk culture	1.5	2.0	1.5	1.5	1.5	1.0
	Employee and contractor security	2.0	3.0	2.0	2.0	2.0	2.0
3	Integrate cyber-resilience into enterprise-wide management and governance processes	2.2	3.0	1.3	2.0	1.8	2.7
	Product security	1.0	3.0	1.5	2.5	1.5	2.0
	Vendor and other third-party mgmt.	2.0	2.6	2.0	1.8	1.5	2.0
4	Integrated incident response across business functions, enhanced by realistic testing	1.5	2.5	1.5	1.5	2.0	2.0
	Risk reporting and metrics	2.3	2.3	2.3	1.2	1.6	2.0
	Organization structure and roles	1.0	1.5	0.0	1.0	1.5	0.5
5	Develop deep integration of security into the technology environment to drive scalability	2.0	2.5	n/a	2.0	2.0	2.0
	Cloud security	2.0	1.5	0.0	0.0	0.0	1.5
	Secure app. and systems dev.	2.0	3.0	2.5	2.5	1.5	2.0
6	Provide differentiated protection for most important assets	1.2	2.5	1.0	1.2	0.5	1.5
	Secure architecture	4.0	2.0	2.0	3.0	2.0	2.0
	Logical security	1.5	3.3	1.5	2.0	2.0	1.3
7	Deploy active defenses to respond to emerging attacks in real time	2.7	4.0	3.0	3.7	3.0	2.0
	Physical security	2.0	3.0	3.0	3.0	3.0	3.0
	Policies and standards	1.0	2.0	2.0	0.0	1.0	1.0
	Program and project management	3.0	3.0	3.0	3.0	3.0	3.0
	Cyber intelligence and vulnerability awareness	3.0	3.0	3.0	3.0	3.0	3.0
	Monitoring and analytics						

McKinsey & Company | 14



Services you could leverage: CyberFit, the healthcare cybersecurity services provider Utility

What is the health-care 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** in the healthcare cyber security value chain
- 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

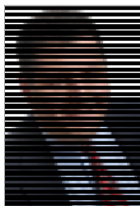
McKinsey & Company | 16

Services CyberFit will offer


	Description of MVP service	MVP Availability
Policy & Regulatory updates	<ul style="list-style-type: none"> Periodic updates (emails/ portal) to all subscribing members on regulation, legislation, rulings etc. relating to healthcare Service to focus on events in North America and select countries Legal analysis, and updates beyond standard published reports 	Q3, 2016
Organizational benchmarks	<ul style="list-style-type: none"> Online assessment on several dimensions of digital resiliency Benchmarks and comparisons with healthcare/ other industry peers Standard reports with assessment history and maturity trail 	Q3, 2016
3rd-party risk assessments	<ul style="list-style-type: none"> Library of assessments based on common assessment criteria applied to assessments from various contributors Standard risk assessments for industry best vendors, and custom assessments based on subscriber specific criteria 	Q3, 2016
Vulnerability & pen testing	<ul style="list-style-type: none"> Penetration testing/ Vulnerability scanning based on Utility develop standards Best-in-class recommendation based on test and analysis and roadmap to achieve better resiliency 	Q3, 2016
Shared SOC	<ul style="list-style-type: none"> Shared operations center providing key security capabilities (e.g., incident response, malware analysis, forensics) Vendor provided shared SOC, potentially at a low-cost location 	Q4, 2016

McKinsey & Company | 17

Questions?



James_Kaplan@mckinsey.com
@jmk37



Venky_anant@mckinsey.com

McKinsey & Company | 18
