Cybersecurity Challenge Prompt
AIS Student Leadership Conference @ FIU

The Cybersecurity Budget Challenge: Optimizing Cybersecurity Spending under Budget Constraints

Prepared by Sebastian Schuetz and Louis Lerman

November 18, 2022

(Updated hyperlinks, Feb 15th 2023)

Scenario

The Call

It was a sunny Tuesday afternoon in October 2022 when Brooks Boots, Chief Information Officer (CIO) of Biscayne Medical Center (BMC), called Tyler Meyers, her Chief Information Security Officer (CISO). Her voice made it clear that the matter was urgent:

> *Tyler, I just came out of a board meeting, and I need to cut costs. I know you have ideas on how to bolster our security posture, and that this is not what you want to hear, but I'm telling you the facts. I need you to come up with a minimum spend budget. Also, please remember that we are about to transition our legacy EMR system into the Cloud, so please consider that in your budget.*

Boots, the new CIO of BMC, had just initiated a Cloud-first strategy for all BMC, starting with the Electronic Medical Record (EMR) system. In 2004, under the umbrella of the Bush administration's initiative to fuel widespread adoption of EMR, BMC had heavily invested into EMR. The system was once upgraded in 2014, costly to maintain and provision, and now nearing the end of its second ten-year support cycle. Brooks plan was to move the system to a Cloud-based infrastructure. Tyler responded:

> *Brooks, I get it. What do you need from me?*

Brooks explained:

> *I need you to help me cut costs without sacrificing cybersecurity. Let me know your budget needs for next year. I need to know what it will cost us to secure our systems, including the upcoming Cloud-based EMR, to regulatory standards.*

Tyler summarized:

> *You need me to come up with a number. Alright. By when?*

Brooks:

> *I need more than just a number. I also need your plan about staffing, systems, vendors, partners, insurance, the whole thing. Make sure to only propose and budget for the expenses that we really need. I will need to justify each expense to the board. The next board meeting is next week Monday. Let me know by Friday.*

Background on Biscayne Medical Center

BMC is a publicly funded hospital located in Miami, South Florida. Founded in 1964, as a small medical center, it has since steadily expanded. Since 2017, BMC's campus comprised 55 beds, 4 ICU beds, a 4-bed surgical unit, 24/7 emergency services, its own laboratory and radiology. At its campus, BMC employs over 100 doctors, 230 nurses, 20 administrators, and 100 supporting staff.

Since 2019, BMC has seen a steady growth in revenues, with recent growth being largely fueled by CARES Act relief funding provided in response to the COVID pandemic. However, despite growing revenues, BMC's operational profit margin has been shrinking. What was a healthy and industry-leading 7% in 2019 has been reduced to 5% in 2021, with a downward outlook for 2022 (see Appendix A. Profit and Loss Statements). In addition to the pressure on BMC's profit margin, environmental uncertainties related to the future provision of relief funding and a possible recession in the economy create an uncertain outlook.

In light of these trends, and to ready BMC for what is to come, BMC's Board of Directors has tasked management to cut costs. It is with this background that Brooks made the call to Myers, asking for the anticipated cybersecurity budget and to only budget for what is necessary.

Initial Considerations

When Meyers hung up on the phone, the challenge was clear. There were many items that, expecting a larger budget given the recent increases in cyberattacks, Meyers had planned for. Meyers aligned BMCs security posture to follow a defense-in-depth strategy, and hence used this model as a guideline for deciding on BMCs security measures. To get an overview of all of the expected spending, Meyers started to note down the things that were being considered (see

Table 1 below) in addition to the two security analysts (Aurelia Rodriguez and Denzel Williams) currently on staff which also were also paid for from Meyers' budget.

Table 1. *Items Taylor Meyers Was Already Considering For 2023*

Category	Expenses	Quantity	Description	Estimated Annual Cost
Service (procured from third party)	IT Security Audit	1	Professional audit of security posture and compliance with regulatory requirements	$10,000
	Security Education & Awareness Training	500 (all doctors, nurses, and other staff)	Training on security threats (such as phishing), compliance requirements and cyber hygiene	$25,000
	Ransomware insurance	1	Will cover the ransom pay in a ransomware event. Requires 2FA and EDR. Limit $1,000,000. (Higher limits are possible but will increase the fees in a linear fashion).	$10,000
	Data breach insurance	1	Will cover legal fees and remediation for data breaches (leak/theft of PHI). Limit $1,000,000. (Higher limits are possible but will increase the fees in a linear fashion).	$5,000
	Penetration testing	1	Will identify weak spots in BMCs security posture	$25,000
	Incident response retainer	1	24/7/365 incident response services in case of a cybersecurity incident	$15,000
	Threat monitoring service	1	24/7/365 monitoring services of security environment	$10,000
Software & Licenses	Antivirus	243 (all doctors, nurses, and other staff)	Identifies viruses on workstations	$12,150
	Intrusion detection systems	1 seat	Detects malicious traffic	$8,000
	Endpoint Protection and Response Software	500 (all doctors, nurses, and other staff)	Continuous end-point monitoring and automated response.	$20,000
	Multi-factor Authentication	500 (all doctors, nurses, and other staff)	Enables second-factor authentication during log-ons	$3,000
People	Security analyst	1	Monitoring for malicious traffic, reporting Risk assessment Security training	$80,000

	Network & Systems specialist	1	Computer maintenance & vulnerability management, supporting firewall and anti-virus software and other technologies	$90,000

With the typical security IT budget ranging between 5% to 7% of total IT spend, Meyers was anticipating a budget in the range between $175,000 to $250,000. However, given the budget pressures on Brooks, Meyers was sure that a lower spend would be appreciated if it could be achieved without compromising the security of BMC's information systems. He also knew that if the high-end of the budget range was overshot, Brooks would require rock-solid justifications. In reviewing the items, Meyers already realized that doing all would exceed the high-end of the budget expectations. Thus, now more than ever, Meyers would need to prioritize and shuffle around to achieve their security goals.

The EMR Migration to the Cloud

In addition, Meyers now had to figure out what else would be needed to secure the new EMR system to the Cloud. The EMR system was a software platform for the electronic entry, storage, and maintenance of digital medical data. EMR systems thus contain all confidential medical information. At the time of procurement, the system used to be industry leading. Currently installed on an on-premise Citrix cluster and connected to an on-premise Oracle database cluster Oracle, the system could be accessed via applications installed on the 243 PC workstations and 59 tablets provided to hospital staff, doctors, nurses, and administrators. Every doctor and administrator had their own workstation, and nurses and supporting staff shared theirs. Tablets were shared by doctors and nurses and mainly were used to present information to patients. The EMR system received frequent updates that, however, sometimes broke the integration with other hospital applications (i.e., billing, pharmaceuticals, radiology) and thus required extensive validation and testing before deployment.

Brooks strategy was to forgo the on-premises Citrix cluster for a Citrix Cloud solution. Citrix Cloud is a PaaS that can be partnered with any IaaS provider. To that end, Brooks wanted to pair Citrix Cloud with the IaaS services of a local data center operator in Miami. As part of the migration, the EMR system would also be upgraded to a web-based client that can be accessed via encrypted HTTPS. This would reduce the need for VPNs going forward but potentially require investments into multi-factor authentication and/or single sign-on. Starting with the EMR system, if proven a success, Brooks planned for later systems to follow, eventually reducing the need for on-premises infrastructure.

The Challenge

Brooks had tasked Meyers to design a minimal spend budget for 2023 that did not compromise BMC systems' security and compliance. It is your task to rise to this challenge. Step in the shoes of Meyers and design a budget for a cybersecurity function (people, process, technology) that suffices for protecting against common and anticipated cybersecurity threats and that considers regulatory compliance requirements. Your plan should consider the needs after the EMR-Cloud migration. Your plan should detail an overall budget, each item, and a justification for each item.

In preparing your plan, consider the following questions and resources:

1) What are the priorities for BMC's cybersecurity function, and how could you justify/identify the priorities? What are the most common threats and most severe risks to hospitals like BMC?
2) Has Meyers considered all options, or are there more items that Meyers missed?
3) What does Meyers need to secure the EMR system provisioned through the Cloud?
4) Do some of the items serve redundant purposes? Do they overlap in their function?

5) Are there items whose cost can be reduced?

6) What items are required due to regulatory requirements? Which regulations apply?

7) Can some items be sourced cheaper by using internal resources, or from external service providers, or even partially internal/external?

Among other resources that you can find, some of the following may be useful for your preparation. Use these and others to guide your decisions.

1. Profit and Loss statement (see Appendix A)

2. IT Application Inventory (see Appendix B)

3. Current ISP (see Appendix C)

4. Current Organizational Chart (see Appendix D)

5. HIPAA Regulations (Link)

6. Healthcare Data Breach Cost (Link)

7. Top 10 Cybersecurity Challenges (Link)

8. Healthcare Data Breach Trend Report (Link)

9. Cloud Security Report (Link)

10. Risk of Shadow IT in Healthcare (Link)

11. Defense in Depth (see Appendix E)

Appendix A. PROFIT AND LOSS STATEMENTS

	2019	2020	2021
Revenue			
Net patient service revenue	$56,410,505	$60,011,175	$61,867,191
CARES Act provider relief funds		$5,312,084	$5,365,741
Other revenue	$847,199	$891,788	$948,711
Total	*$62,091,700*	*$66,215,047*	*$68,181,643*
Expenses			
Salaries and wages	$23,559,772	$25,889,860	$28,141,152
Employee benefits	$8,149,113	$8,401,148	$8,937,391
Supplies	$11,201,145	$12,175,158	$12,298,139
Utilities	$780,991	$796,929	$813,193
Purchased services	$9,253,975	$10,282,194	$10,401,261
Depreciation and amortization	$3,641,312	$3,951,215	$4,619,284
Total operating expenses	*$56,586,30*	*$61,496,504*	*$65,210,420*
Income from operations, net	$5,505,392	$4,718,543	$2,971,223

APPENDIX B. IT APPLICATION INVENTORY

Enterprise Applications
Inpatient Billing
Imaging software (radiology)
Inpatient registration
EMR system
Pharmacy software
Ambulatory EMR
Scheduling software
Outpatient billing
Timekeeping
Electronic faxing
Supply inventory management
Payroll
Email/Office
VPN

APPENDIX C. EXCERPTS FROM BMC'S CURRENT INFORMATION SECURITY POLICY

Malware Policy

All computer devices connected to the BMC network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without IT approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Email

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on BMC's computer systems. BMC can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by BMC, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to BMC systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Telework & Remote Access Policy

Authorized personnel are allowed to connect to BMC's computer networks using their own devices (PCs, mobile phones).

When connecting from remote, authorized personnel must use a VPN to connect to BMC's computer systems and applications before using them. A VPN is a secure "tunnel" that connects the teleworker's device to the organization's network. Once the tunnel has been established, the teleworker can access many of the organization's computing resources through the tunnel. The VPN ensure the security of the transaction through encryption. Each employee must use the VPN to connect to BMC's computer systems and applications before using them.

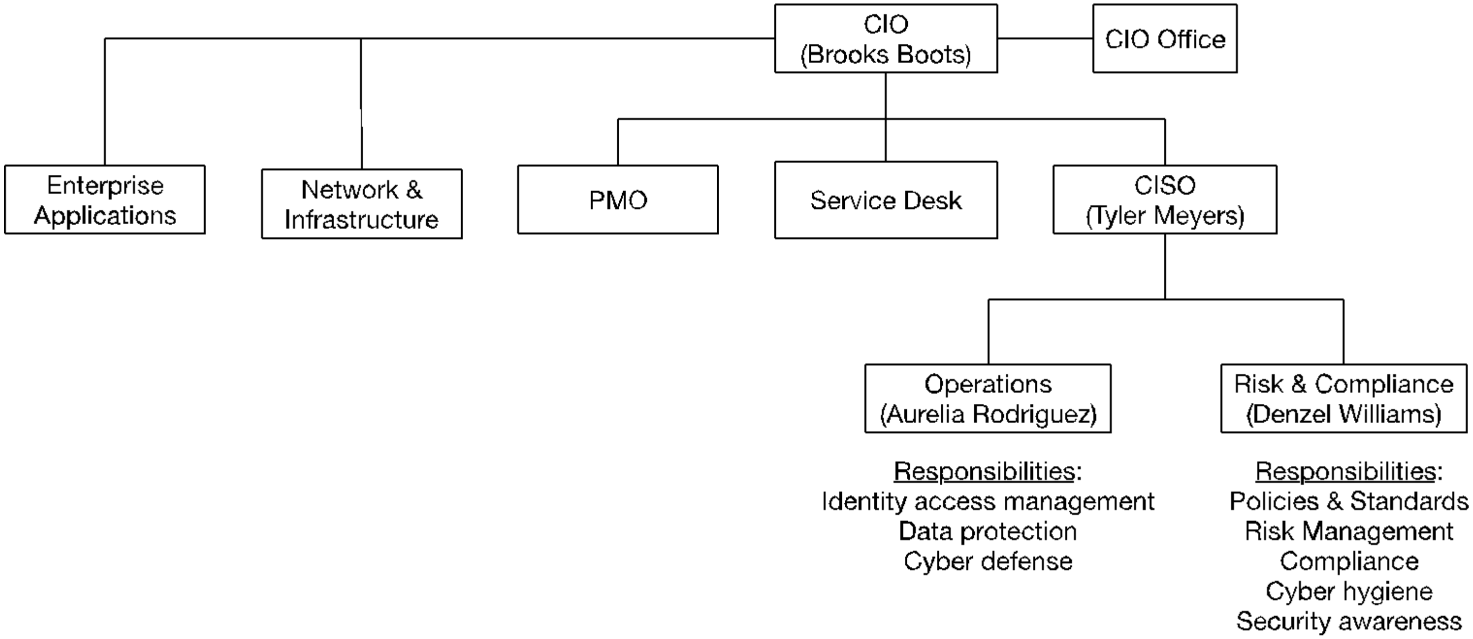
BYOD Policy

BMC grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. Company ABC reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of BMC's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

BMC employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

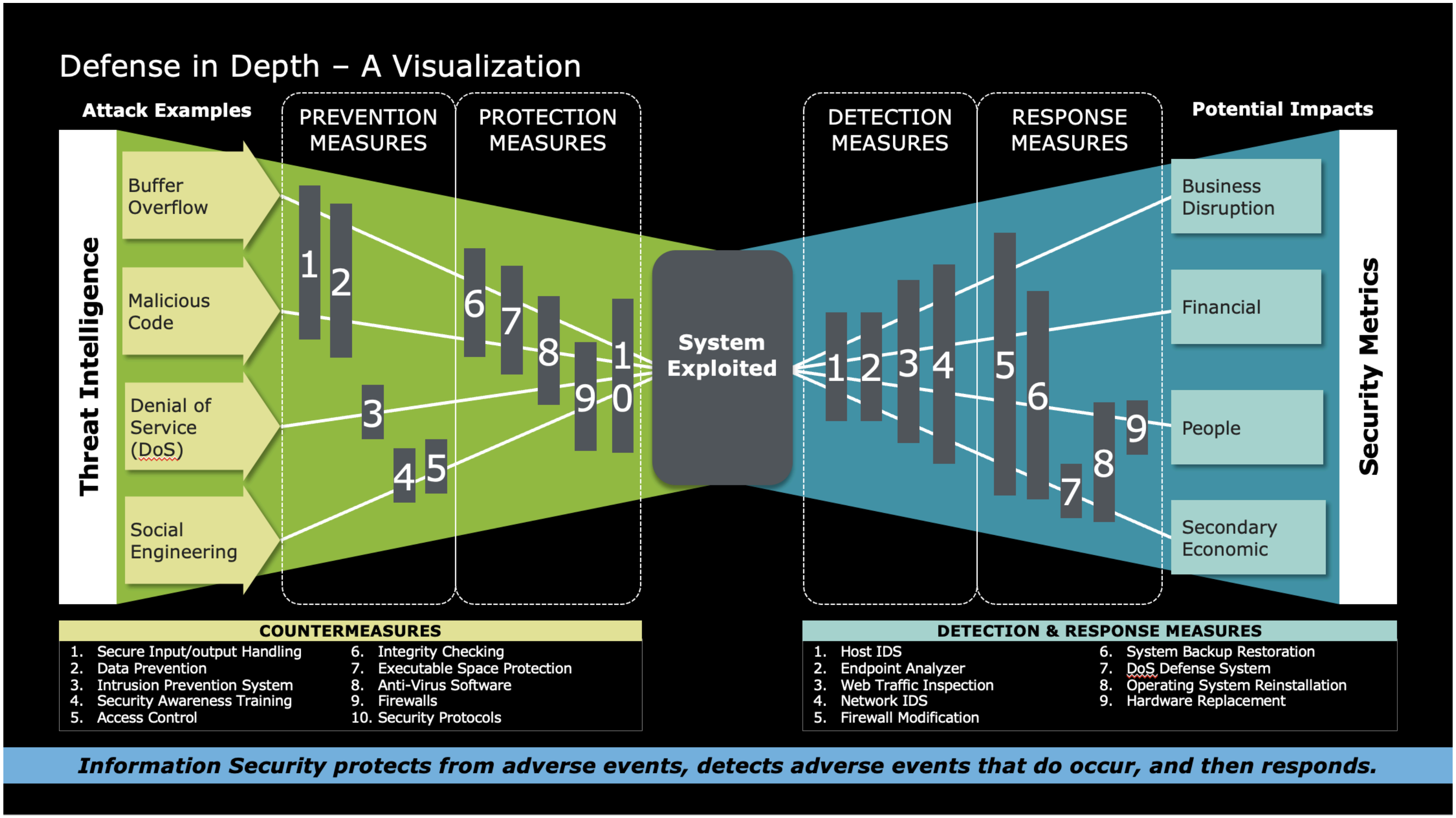
APPENDIX D. ORG CHART OF IT FUNCTION



Responsibilities:
Identity access management
Data protection
Cyber defense

Responsibilities:
Policies & Standards
Risk Management
Compliance
Cyber hygiene
Security awareness

Appendix E. Defense IN DEPTH



Defense in Depth – A Visualization

COUNTERMEASURES

1. Secure Input/output Handling
2. Data Prevention
3. Intrusion Prevention System
4. Security Awareness Training
5. Access Control
6. Integrity Checking
7. Executable Space Protection
8. Anti-Virus Software
9. Firewalls
10. Security Protocols

DETECTION & RESPONSE MEASURES

1. Host IDS
2. Endpoint Analyzer
3. Web Traffic Inspection
4. Network IDS
5. Firewall Modification
6. System Backup Restoration
7. DoS Defense System
8. Operating System Reinstallation
9. Hardware Replacement

Information Security protects from adverse events, detects adverse events that do occur, and then responds.