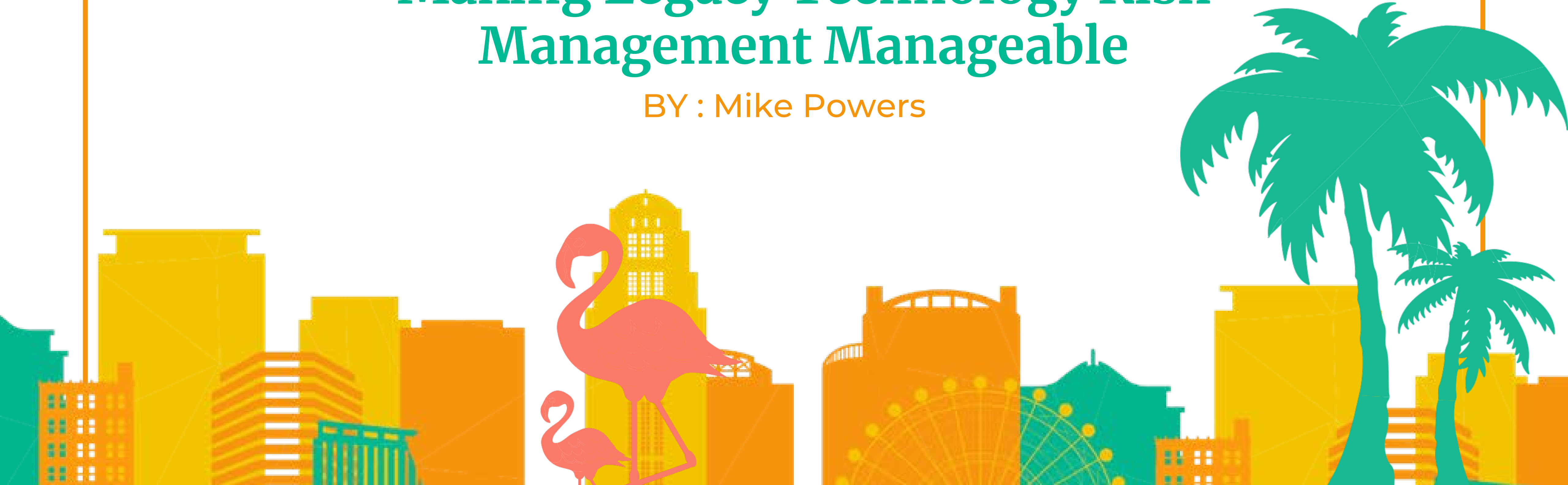
MDEXPO
Orlando, FL • October 29-31, 2023

Legacy Technology 411:

Making Legacy Technology Risk Management Manageable

BY : Mike Powers



In March 2023, the HSCC published the HIC-MaLTS

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Manage Risks

Secure Medtech

Health Industry Cybersecurity

Managing Legacy Technology Security (HIC-MaLTS)

MARCH 2023

The HIC-MaLTS is 115 pages…

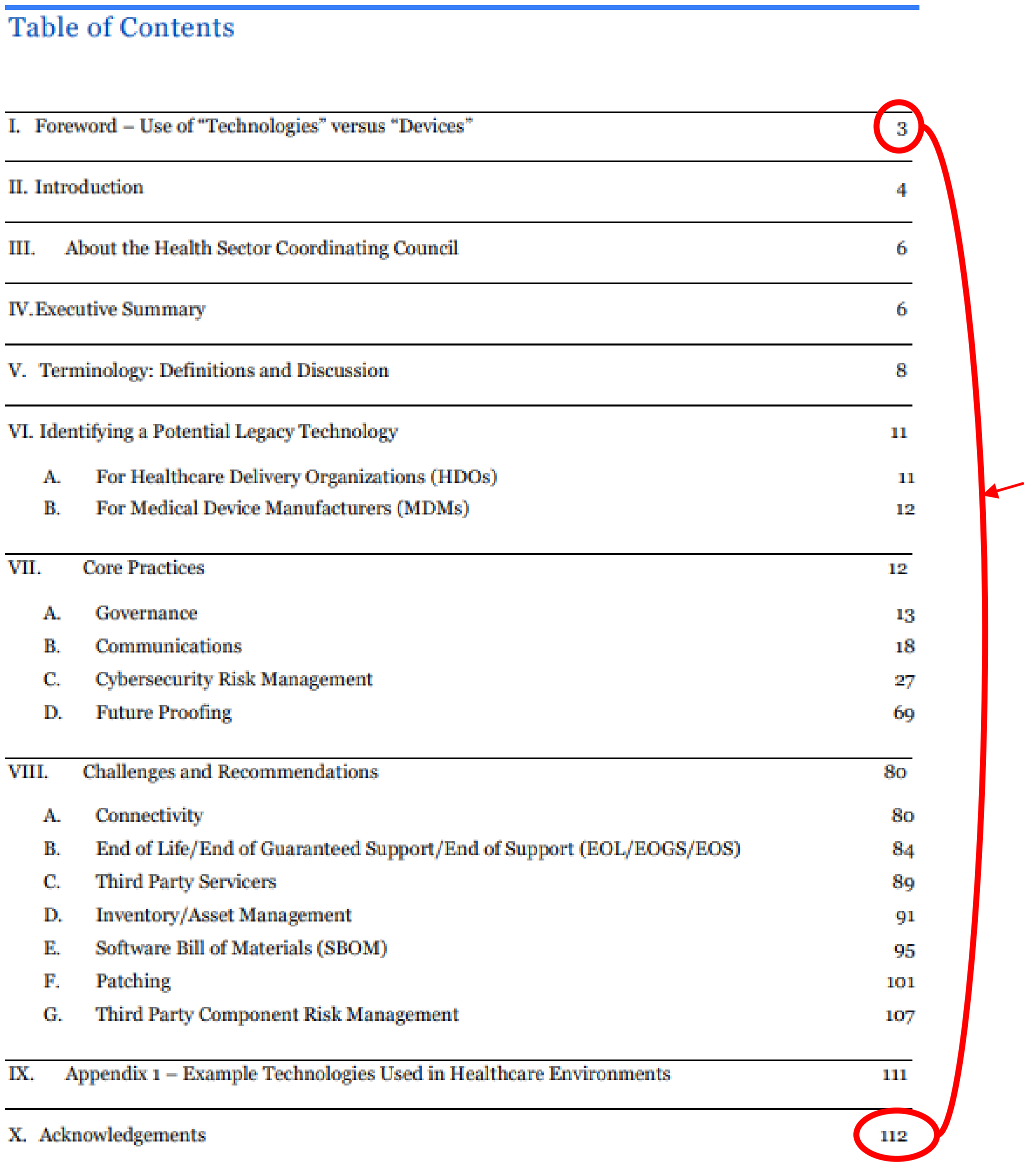


Table of Contents

(That's a lot of pages!)

So let’s take a step back…

…and ask what we really want to do.

I am an HDO, MDM, 3rd Party and I want to:

Avoid acquiring legacy technologies, or those that might become legacy quickly or unexpectedly

Protect the legacy technologies that I already have

Comply with SBOM Requirements (and take advantage of SBOM benefits)

Manage my non-legacy technologies to keep them non-legacy as long as possible

Make a smart, risk-informed decision about whether I need to replace a given legacy technology in my environment

Support my customers in managing technologies to keep them as non-legacy as long as possible

Design, deploy, and maintain secure and securable technologies

The HIC-MaLTS Can Help With All That!

Goal: Avoid Acquiring Legacy Technologies, or Those That Might Become Legacy Quickly or Unexpectedly

- How do I determine whether a technology may be “legacy”?
  - *Identifying a Potential Legacy Technology (pgs. 11-12)*
- How do I make sure I understand what terms/characteristics a technology may have, to know whether it might be “legacy”?
  - *Terminology (pgs. 8-9)*
- How do I develop a strategy around my organization’s technology acquisitions and maintenance?
  - *Defining a Legacy Technology Risk Management Strategy (pg. 14)*
- How do I draft and negotiate my contracts to address legacy technology risks?
  - *Considerations for Legacy Technology Communications (pgs. 19-26)*
- How should I assess a technology for legacy risks?
  - *Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Product Assessment Stage (pg. 33-34)*
- How should I acquire technologies to avoid legacy risks?
  - *Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Acquisition Stage (pg. 35)*

Goal: Manage my non-legacy technologies to keep them non-legacy as long as possible

- How do I make sure that I know, understand, and am acting on my technologies' various "ages"?
  - *Developing a Lifecycle Management Plan (pg. 16)*
- How do I manage my non-legacy technologies to keep them secure and securable for as long as possible?
  - *Managing Future Legacy Technologies (pgs. 31-40)*
- How do I implement technologies in my environment to manage legacy risks?
  - *Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Implementation Stage (pg. 36)*
- How do I support technologies in my environment to manage legacy risks?
  - *Recommendations to Address Legacy Risk Management throughout Technology Lifecycles: Support/Maintenance Stage (pg. 37)*
- How can I keep up with patches?
  - *Patching Lifecycle Recommendations (pgs. 50-69)*
  - *Patching (pgs. 101-107)*

Goal: Protect the Legacy Technologies I Already Have

- How do I identify a potential legacy technology?
  - *Identifying a Potential Legacy Technology (pgs. 11-12)*
- How do I decide how much “risk” I can handle?
  - *Establishing a model and criteria for risk tolerance (pg. 15)*
- How do I manage the risks of my current legacy technologies?
  - *Managing Current Legacy Technologies (pg. 28)*
- My organization is having trouble with certain cybersecurity challenges. How do I:

Assess whether I can/should connect technologies to my network, that may not have been designed for that purpose?

- *Connectivity (pgs. 80-84)*

Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?

- *End-of-Life/End-of-Support (pgs. 84-89)*

Understand how and when I may want to leverage third-party support servicers?

- *Third Party Servicers (pgs. 89-91)*

Fully identify, track, and manage my inventory of digital technologies?

- *Inventory/Asset Management (pgs. 91-95)*

Understand, produce, and effectively use SBOMs?

- *SBOM (pgs. 95-101)*

Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?

- *Patching (pgs. 101-107)*

Understand the benefits and risks that third party components may pose, and what I may do to effectively manage them?

- *Third Party Component Risk Management (pgs. 107-112)*

Goal: Make a Smart, Risk-Informed Decision About Whether I Should Replace a Given Legacy Technology

- Legacy technologies exist in my environment, and I recognize that they should be replaced to mitigate or avoid potential cybersecurity risks, but I have very real and very significant competing organizational priorities. How do I make a smart, risk-informed decision about whether I should replace a given legacy technology?
  - *Responsibility Transfer Framework (pgs. 43-50)*

Goal: Comply with SBOM Requirements (and take advantage of SBOM benefits)

- My customers, the government, and my own organization are demanding that I use, produce, and/or consume SBOMs. How do I familiarize myself with what SBOMs are, what they are for, and how I can most effectively take advantage of them?
  - *Communications, SBOM (pgs. 22-23)*
  - *Challenges and Recommendations: SBOM (pgs. 95-101)*

Goal: Support my customers in managing technologies to keep them as non-legacy as long as possible

- How do I understand what support expectations/needs my customers may have, and how to appropriately negotiate them?
  - *Considerations for Legacy Technology Communications (pgs. 19-26)*
- My customers and I both experience challenges related to certain specific technologies or issues. How do I:

Assess whether to connect technologies to networks, that may not have been designed for that purpose?

- *Connectivity (pgs. 80-84)*

Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?

- *End-of-Life/End-of-Support (pgs. 84-89)*

Understand how and when I may want to leverage third-party support servicers?

- *Third Party Servicers (pgs. 89-91)*

Make it easy for my customers to identify, track, and manage my technologies in their environments?

- *Inventory/Asset Management (pgs. 91-95)*

Understand, produce, and effectively use SBOMs?

- *SBOM (pgs. 95-101)*

Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?

- *Patching (pgs. 101-107)*

Understand the benefits and risks that third party components may pose, and what I may do to effectively manage them?

- *Third Party Component Risk Management (pgs. 107-112)*

Goal: Design, deploy, and maintain secure and securable technologies

- How may I design an effective, efficient cybersecurity risk management program?
  - *MDM Risk Management Considerations (pgs. 40-43)*
- How do I proactively consider the potential legacy risks that my technologies may face, and how to design to control for those risks?
  - *Recommendations for Addressing Known Legacy Issues During Threat Modeling (pg. 70-73)*
- How may I design secure technologies that address legacy risks, including the criteria I use to select what software I may use in my technology?
  - *Recommendations for Secure Technology Design, Including Software Selection (pgs. 73-78)*
- How may I facilitate my customers' secure deployment of my technologies?
  - *Recommendations to Facilitate Secure Technology Deployment (pgs. 78-80)*

Goal: Design, deploy, and maintain secure and securable technologies (cont’d)

- My customers and I both experience challenges related to certain specific technologies or issues. How do I:

Assess whether and how to connect technologies to networks, that may not have been designed for that purpose?

- *Connectivity (pgs. 80-84)*

Ensure that I understand, am prepared for, and appropriately manage my technologies as they age?

- *End-of-Life/End-of-Support (pgs. 84-89)*

Understand how and when I may want to leverage third-party support servicers?

- *Third Party Servicers (pgs. 89-91)*

Make it easy for my customers to identify, track, and manage my technologies in their environments?

- *Inventory/Asset Management (pgs. 91-95)*

Understand, produce, and effectively use SBOMs?

- *SBOM (pgs. 95-101)*

Keep up with patches, and design my patching procedures to be as least burdensome and effective as possible?

- *Patching (pgs. 101-107)*

Understand the benefits and risks that third party components may pose, and what I may do to effectively manage them?

- *Third Party Component Risk Management (pgs. 107-112)*

Questions?

MDEXPO

Orlando, FL • October 29-31, 2023

We value your feedback!

Please scan the QR code to submit a survey for this session.

Thank You!