Managing End-of-Life Risk

New York State Cyber Security Conference
June 8th, 2017

Problem Solved.
Agenda

- What is EOL?
- Why should you care? (What’s the risk?)
- EOL Key Risk Indicators
- Common Corrective Actions
- Awareness & Sponsorship
- Questions & Answers

Problem Solved.
What is “End of Life”?

Product status when the manufacturer has discontinued support.

Each manufacturer defines EOL milestones differently.

Typical Milestones:
- EOL/EOS Announcement
- End of Sale
- End of Hardware Support
- End of Software Support
- Final EOL Date
Examples of End of Life

Problem Solved.
The Problem with EOL Assets

Hardware:
- No / limited replacement hardware units & parts

Software:
- No functional enhancements
- No bug fixes
- NO SECURITY PATCHES!!!
What’s the Risk?

Presidential Executive Order

*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

- Known but unmitigated vulnerabilities are among the highest cybersecurity risks
- Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle
How Big is the EOL Problem?

How big is the EOL problem? Very!

According to the Spiceworks 2017 State of IT:

- 52% of businesses have Windows Server 2003 (EOL June 2015)
- 56% of businesses have Windows XP (EOL April 2014)
US Department of Homeland Security

US Computer Emergency Readiness Team

Alert (TA14-069A)

- Computer systems running unsupported software are exposed to an elevated risk to cybersecurity dangers, such as malicious attacks or electronic data loss
- Users may also encounter problems with software and hardware compatibility
- Organizations that are governed by regulatory obligations may find they are no longer able to satisfy compliance requirements
EOL Assets are attractive targets.
Once software products are EOL, likelihood of exploitation and attack greatly increases.

Why?
• Exploits are more easily developed
• Exploits are developed (and executed) with the knowledge that patches will not be made available

It’s like “being subject to zero-day vulnerability forever”.

Problem Solved.
Measuring EOL Risk

Key Risk Indicators (number and percent)

• All EOL Assets
• By EOL Product
• By Asset Type
• By Location
• EOL Assets in Critical Systems
• By Line of Business
Strengthen **Cybersecurity Policies** to reduce EOL risk

- **Require identification and treatment of EOL**

- **Include EOL info in asset inventories**

- **Require proactive maintenance plans**

- **Prevent / control new EOL deployments**
Corrective Actions (cont.)

- Establish risk-based program to reduce / eliminate EOL assets in environment
- Establish plans to proactively maintain systems and replace assets before they are EOL
- Establish ongoing scanning to detect vulnerabilities & EOL assets in environment
- Control new deployments EOL assets
- Establish compensating controls

Problem Solved.
Senior management awareness, support and sponsorship are critical.

Risk assessment report:
- General EOL-related risks
- Extent of problem (narrative & KRI)
- Organizational impact
- Recommended actions & costs

Problem Solved.
Russell Kiernan
Director of Management Consulting &
Security Services

QED National

rkiernan@qednational.com
212-481-6868