Sustainable IT is Secure IT

Building a Resilient and Responsible Digital Future

SEI Secure Software By Design

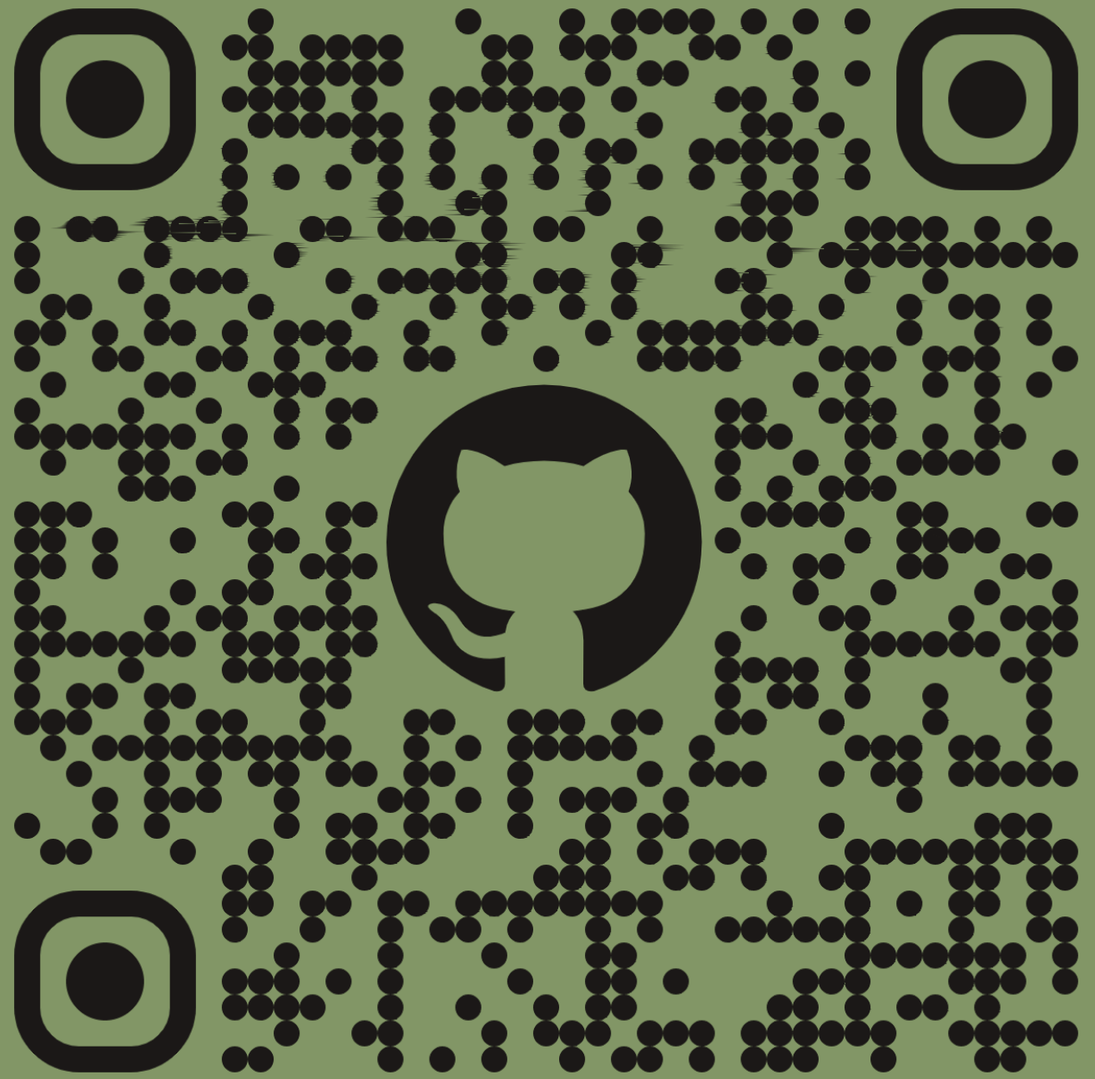
5 August 2024

Making Software Greener, Ltd.

http://MakingSoftwareGreener.com

Link to Slides

https://tinyurl.com/ydv2z4vr



Who am I?

Matt "Kelly" Williams

- Over 35 years IT experien
- International Speaker & Thought Leader in Sustainability, Cloud, and DevOps
- Creator of the Sustainable IT Manifesto
- Green Computing Foundation Advisory Board Member
- Resides in Colorado

Organizations

Green Computing Foundation

Green Computing Foundation

http://GreenComputingFoundation.org

Sustainable IT Manifesto

http://SustainableITManifesto.org

Four Pillars

The Connection Between Sustainability and Security

sustainable practices often lead to more resilient and secure systems

Sustainability:
Meeting current needs without compromising future generations' ability to meet theirs.

Security:
Focus on protecting systems, networks, and data from threats.

Sustainable IT Manifesto

We are uncovering better ways of developing software and hardware by doing it and helping others do it. Through this work, we have come to value...

Energy Efficiency over Raw Performance

Improved Reliability and Reduced Vulnerability

- Example: Google’s energy-efficient data centers

Resource Efficiency over Resource Abundance

Reduced Attack Surfaces and Resource-based Attack Impacts

- Example: Efficient coding practices at Intel

Long-term Sustainability over Short-term Gains

Enhanced System Resilience and Reduced Upgrade Needs

- Example: Microsoft’s carbon negative goal

Holistic Impact Awareness over Siloed Focus

Comprehensive Risk Management

- Example: Cisco’s sustainable supply chain initiatives

Return to Environment over Return on Investment

Stable, Trustworthy Environment

- Example: Apple’s recycling and renewable energy programs

Inclusive Collaboration over Isolated Decision Making

Robust Security Solutions Through Collaboration

- Example: Facebook's collaborative data center designs

Adaptive Planning over Fixed Roadmaps

Quick Responses to Emerging Threats

– Example: Adaptive security planning at Amazon (AWS)

Transparent Reporting over Selective Disclosure

- Trust-building with Stakeholders
- Example: Transparent environmental reporting by Dell

Continuous Environmental Learning over Static Knowledge

Maintaining Robust Defenses with Evolving Knowledge

– Example: Continuous learning initiatives at HP

Community and Ecosystem Wellbeing over Individual Benefits

- Preventing disruptions that affect the larger community

- Example: Community-focused sustainability projects by Lenovo

Eco-friendly Materials over Cheap Alternatives

Longer-lasting Hardware and Reduced Failures

- Example: Eco-friendly materials used by Samsung

Device Longevity over Planned Obsolescence

- Reducing frequency of replacements and new vulnerabilities

- Example: Long-lasting device design by IBM

Practical Steps for Integrating Sustainability and Security

Making Software Greener, Ltd.

http://MakingSoftwareGreener.com

Strategic Goals

- Reduce Energy Consumption
- Minimize Electronic Waste
- Enhance System Resilience
- Promote Ethical Sourcing
- Increase Transparancy
- Foster Continuous Learning

Opportunities

- Innovation and Competitive Advantage
- Risk Mitigation
- Operational Efficiency
- Stakeholder Engagement

Steps

1. Conduct a Sustainability Audit: Assess current energy use, waste production, and sourcing practices.
2. Set Clear Goals: Define specific, measurable sustainability and security goals.

Steps

1. Adopt Energy-Efficient Technologies: Upgrade to energy-efficient hardware and software.
2. Implement E-Waste Programs: Establish programs for the responsible disposal and recycling of electronic devices.

Steps

1. Use Sustainable Materials: Choose eco-friendly and recyclable materials for all hardware components.
2. Enhance Supply Chain Transparency: Work with suppliers to ensure ethical sourcing and traceability.

Steps

1. Regular Training and Education: Provide continuous training on the latest sustainability and security practices.
2. Report Progress: Maintain transparent reporting on progress towards sustainability and security goals.

Overcoming Common Challenges

- Initial Costs
- Resistance to Change
- Lack of Awareness, Consciousness, etc.
- Supply Chain Complexity
- Measuring Impact

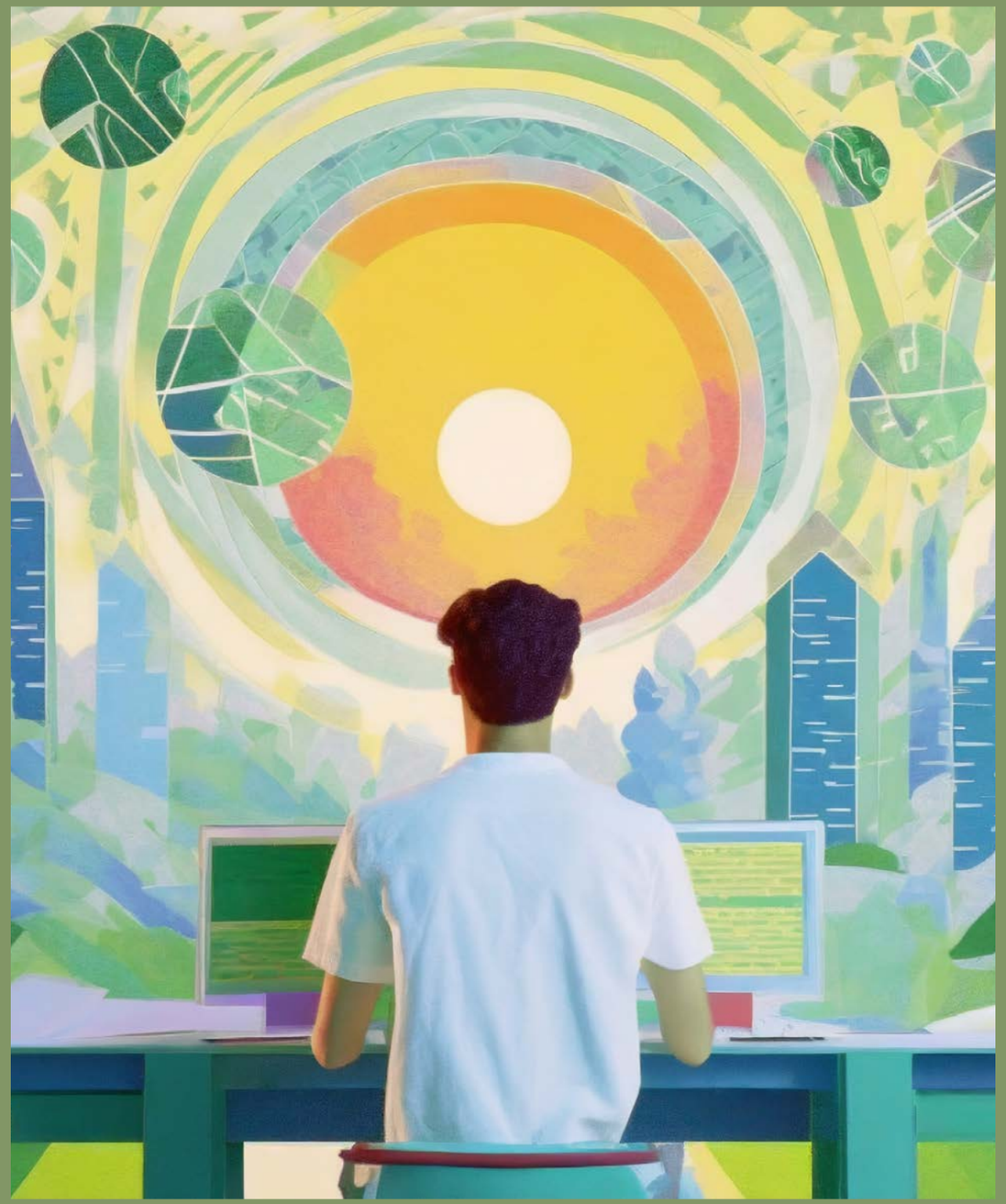
Actionable Tips

- Be Pragmatic
- Start small
- Measure everything
- Engage stakeholders across departments
- "As Above, so Below"
- Tailor the Messaging
- Learn to herd cats

Conclusion

> sustainable practices often lead to more resilient and secure systems

Questions?



Making Software Greener, Ltd.

http://MakingSoftwareGreener.com