digicert®

Public Key Infrastructure:

The Starting Point for IoT Security

Mike Nelson

VP of IoT Security

@mike_k_nelson

What is current state of IoT Security?

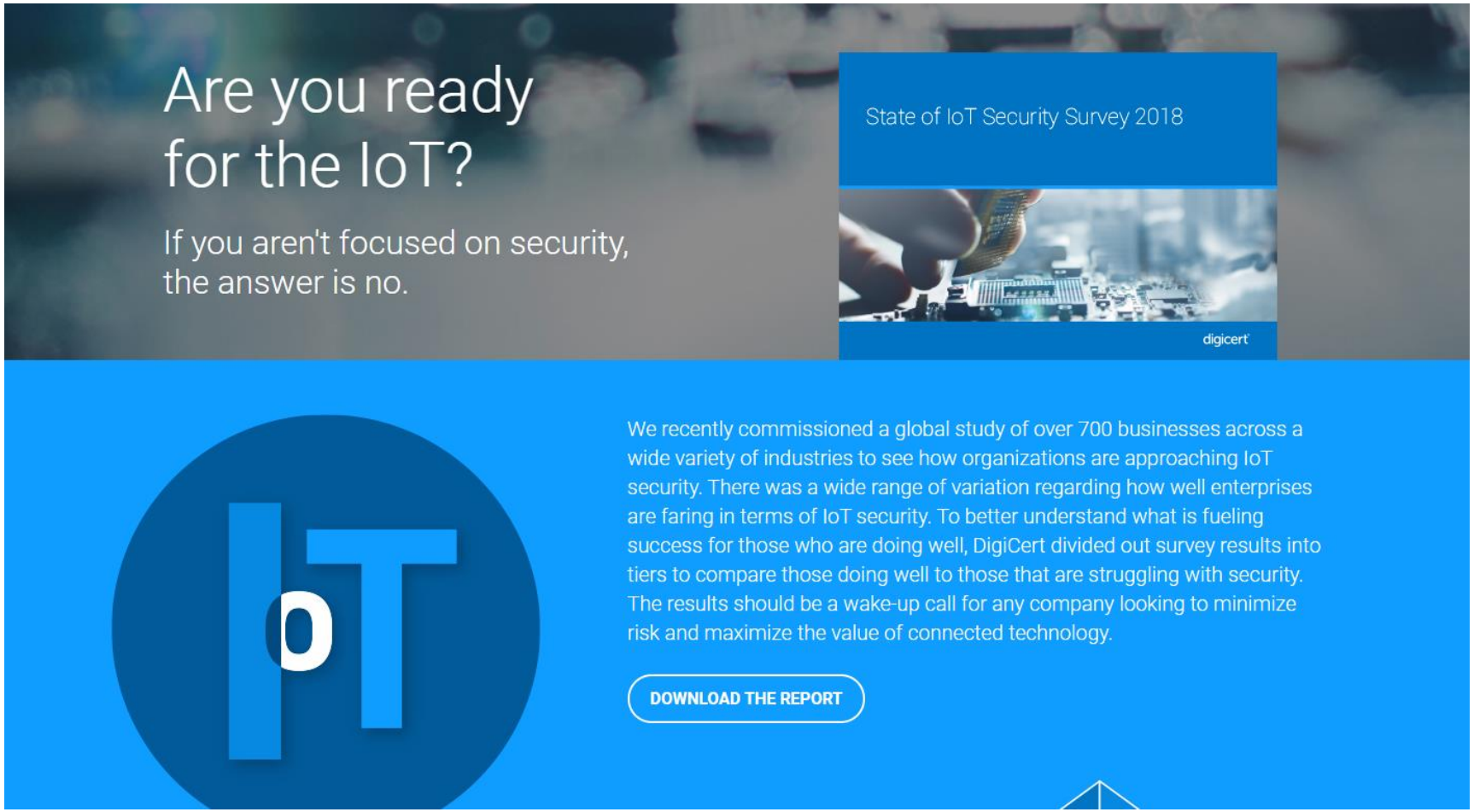
My own incident…

“If you have a $300 head, get a $300 helmet

If you have a $60 head, get a $60 helmet”

- Helmet sales guy

Survey: State of IoT Security



https://www.digicert.com/iotsecurity

Everyone's invested, yet few are prepared

84% of companies are worried about their connected device security

Top IoT priorities for business

INCREASING OPERATIONAL EFFICIENCY

ENHANCING CUSTOMER EXPERIENCE

GROWING REVENUE

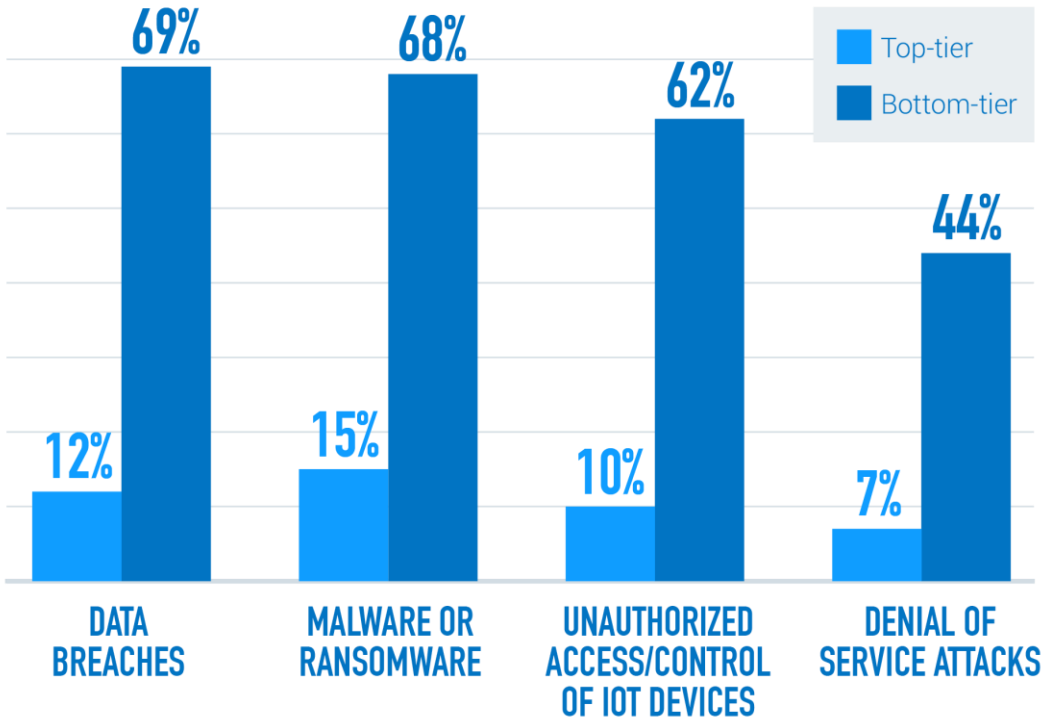
https://www.digicert.com/iotsecurity

The Problem

https://www.digicert.com/iotsecurity

Security Incidents: Top-Tier vs. Bottom-Tier

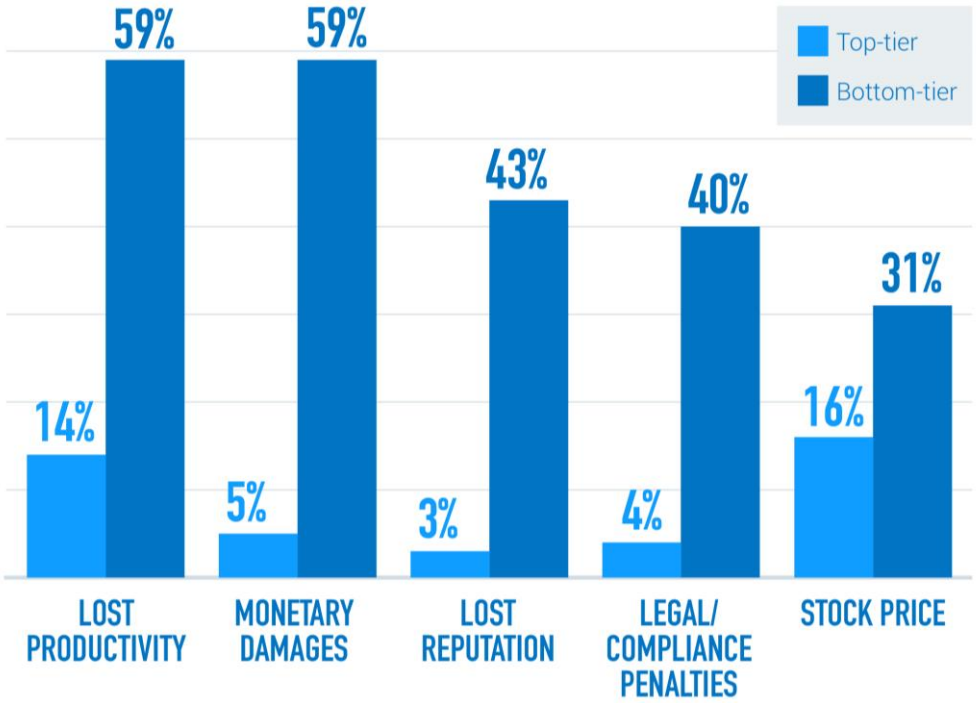
100% of the bottom-tier enterprises experienced at least one security incident.



https://www.digicert.com/iotsecurity

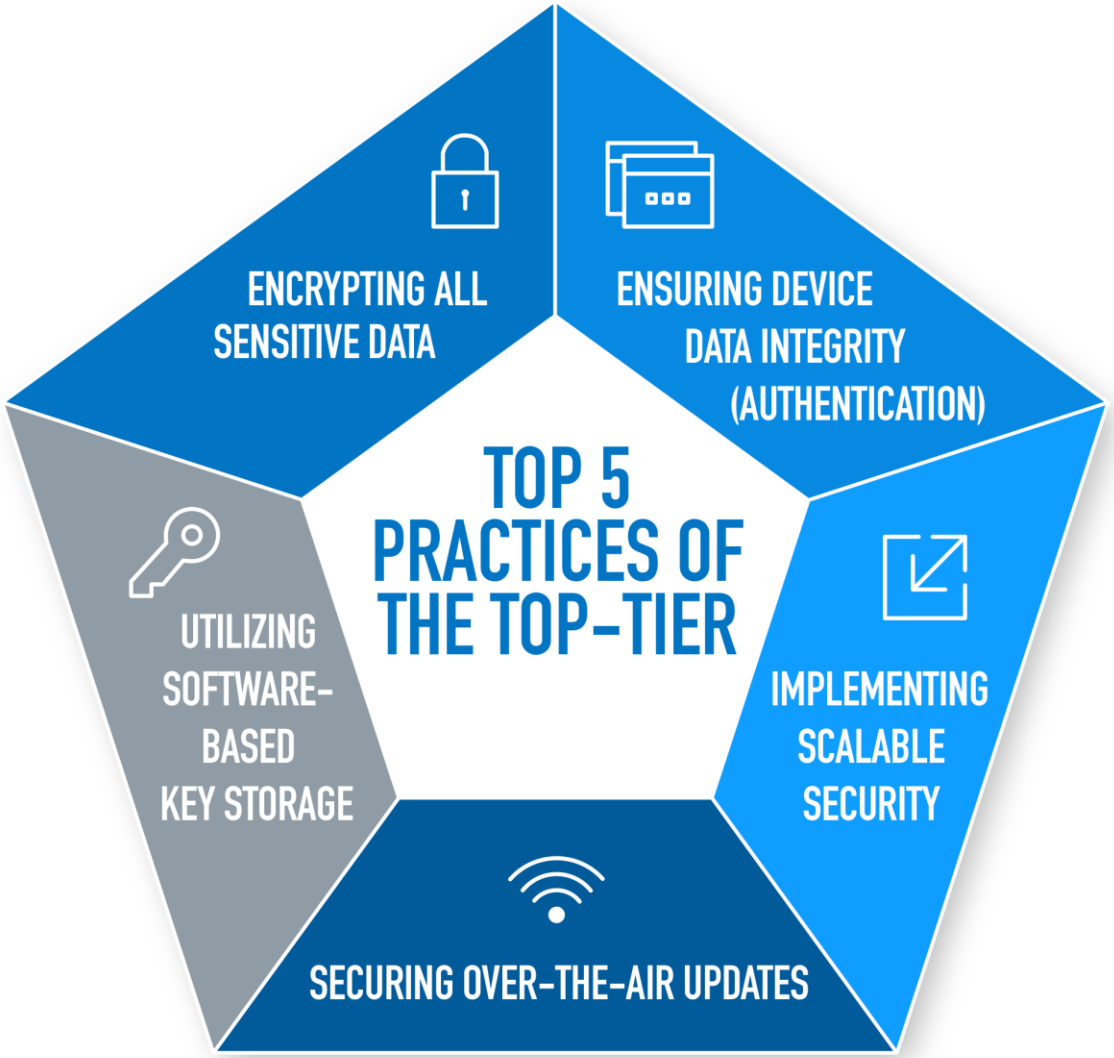
Security Missteps Financial Impact: Top-Tier vs. Bottom-Tier

Average yearly cost in monetary damages: **$384,815**



https://www.digicert.com/iotsecurity

Security Practices of the Top Tier



https://www.digicert.com/iotsecurity

Fundamentals of Good IoT Security

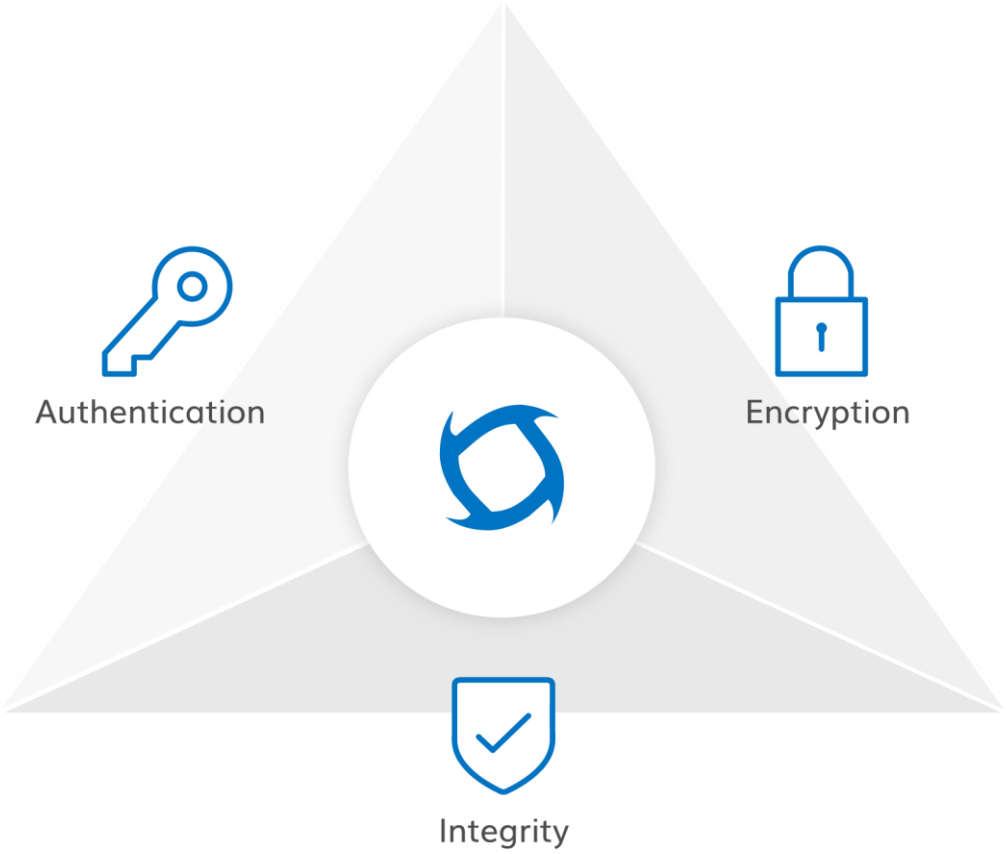
Never trust unauthenticated connections

Never run unsigned code

Never trust unsigned data

Always Encrypt sensitive data

Cornerstones of Public Key Infrastructure (PKI):



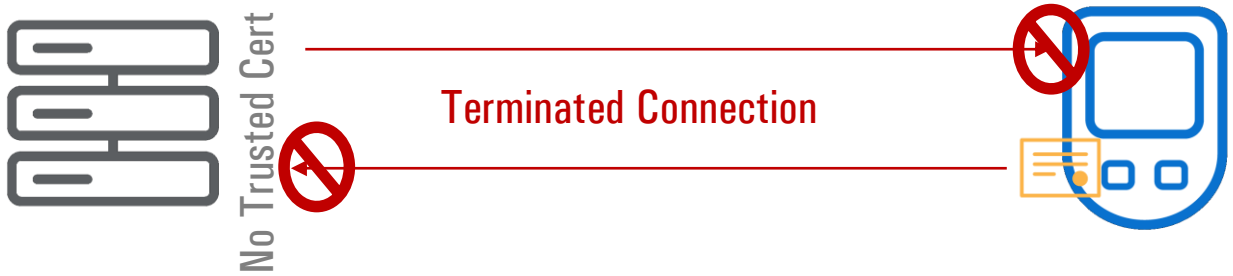
Public Key Infrastructure (PKI)

PKI is a **comprehensive framework** that contains the **set of roles**, **policies**, and **procedures** needed to manage, distribute, create, store, use and revoke **digital certificates**.

Mutual Authentication and Encryption

When connection is made the Device and Service check to make sure:

- ✓ The certificate is signed by trusted root
- ✓ The certificate is signed by a trusted intermediate CA
- ✓ The current date w/in the validity period of the certificate
- ✓ The certificate has not been revoked



When connection is made the Device and Service check to make sure:

- ⊘ The certificate is signed by trusted root
- ⊘ The certificate is signed by a trusted intermediate CA
- ⊘ The current date w/in the validity period of the certificate
- ⊘ The certificate has not been revoked

PKI Considerations / Complexities

Root of trust hierarchy

Certificate Profiles – validity periods

Secure storage of private keys

Certificate provisioning

Certificate management system

Certificate Policy (CP) document

Certificate Practice Statement (CPS)

Take Action

1. Build security into your product life cycle
2. Understand the risk of your devices
3. Authenticate all connections to your device
4. Encrypt sensitive data coming to or going from your device
5. Use digital signatures and code signing to ensure integrity of data packages

digicert®

Thank you

Mike Nelson

VP of IoT Security

Mike.Nelson@digicert.com

@mike_k_nelson