



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...

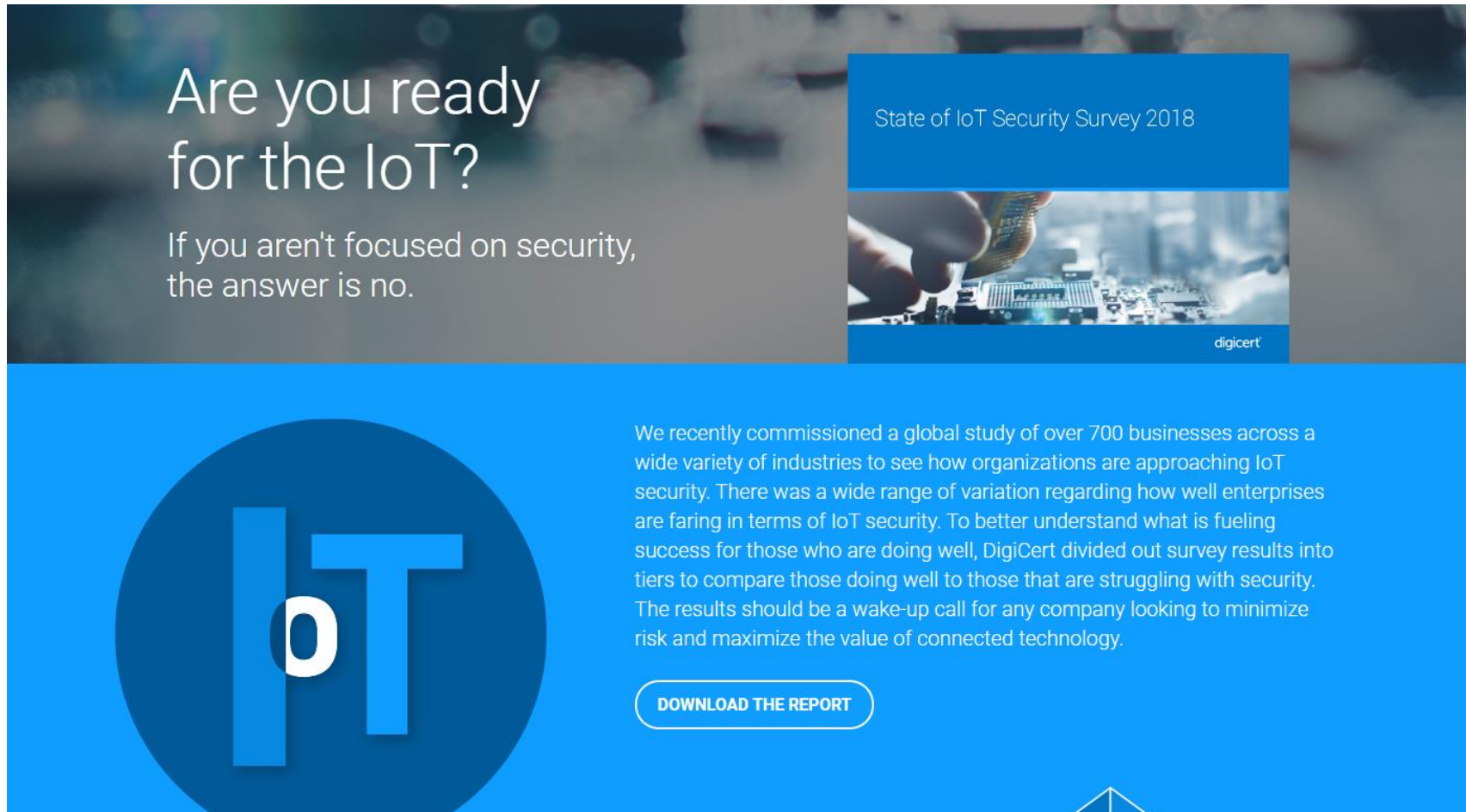


"If you have a \$300 head, get a \$300 helmet

If you have a \$60 head, get a \$60 helmet"

- Helmet sales guy

Survey: State of IoT Security



Are you ready
for the IoT?

If you aren't focused on security,
the answer is no.

State of IoT Security Survey 2018

digicert

IoT

We recently commissioned a global study of over 700 businesses across a wide variety of industries to see how organizations are approaching IoT security. There was a wide range of variation regarding how well enterprises are faring in terms of IoT security. To better understand what is fueling success for those who are doing well, DigiCert divided out survey results into tiers to compare those doing well to those that are struggling with security. The results should be a wake-up call for any company looking to minimize risk and maximize the value of connected technology.

[DOWNLOAD THE REPORT](#)

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



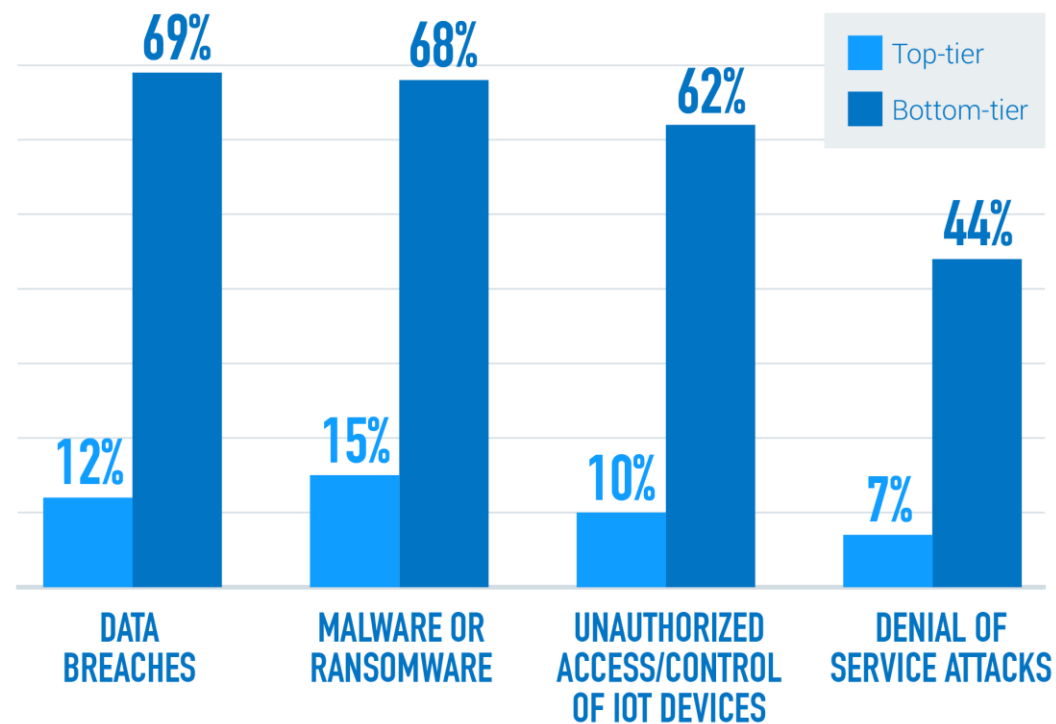
GROWING
REVENUE

The Problem



Security Incidents: Top-Tier vs. Bottom-Tier

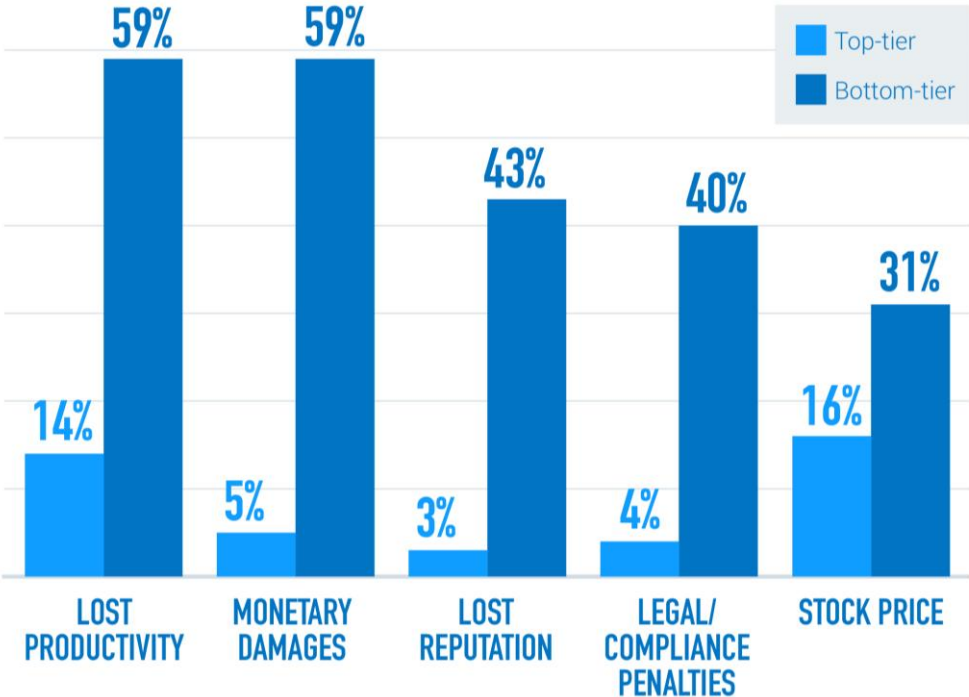
100% of the bottom-tier enterprises experienced at least one security incident.



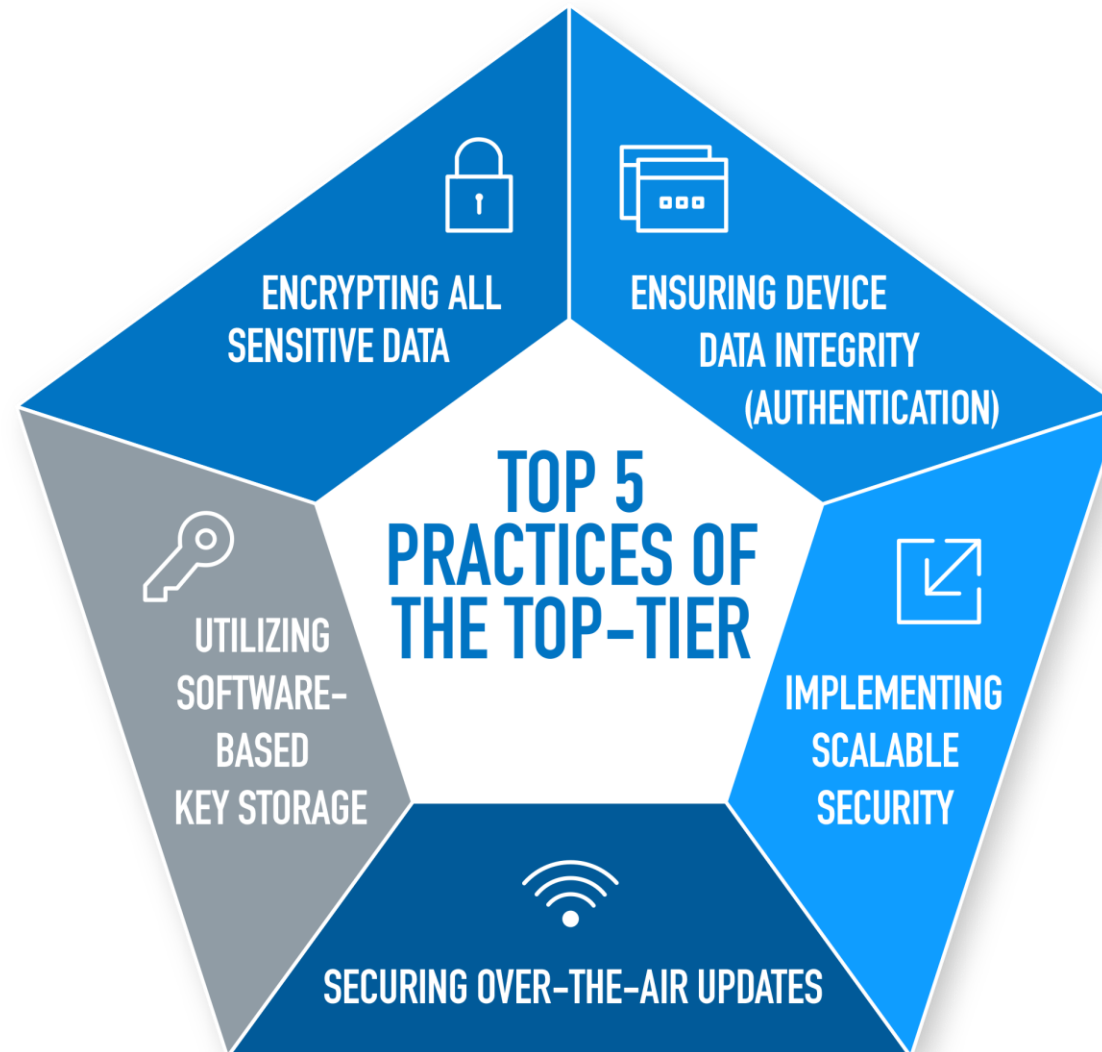
Security Missteps Financial Impact: Top-Tier vs. Bottom-Tier

Average yearly cost in
monetary damages:

\$384,815



Security Practices of the Top Tier



Fundamentals of Good IoT Security

Never trust unauthenticated connections

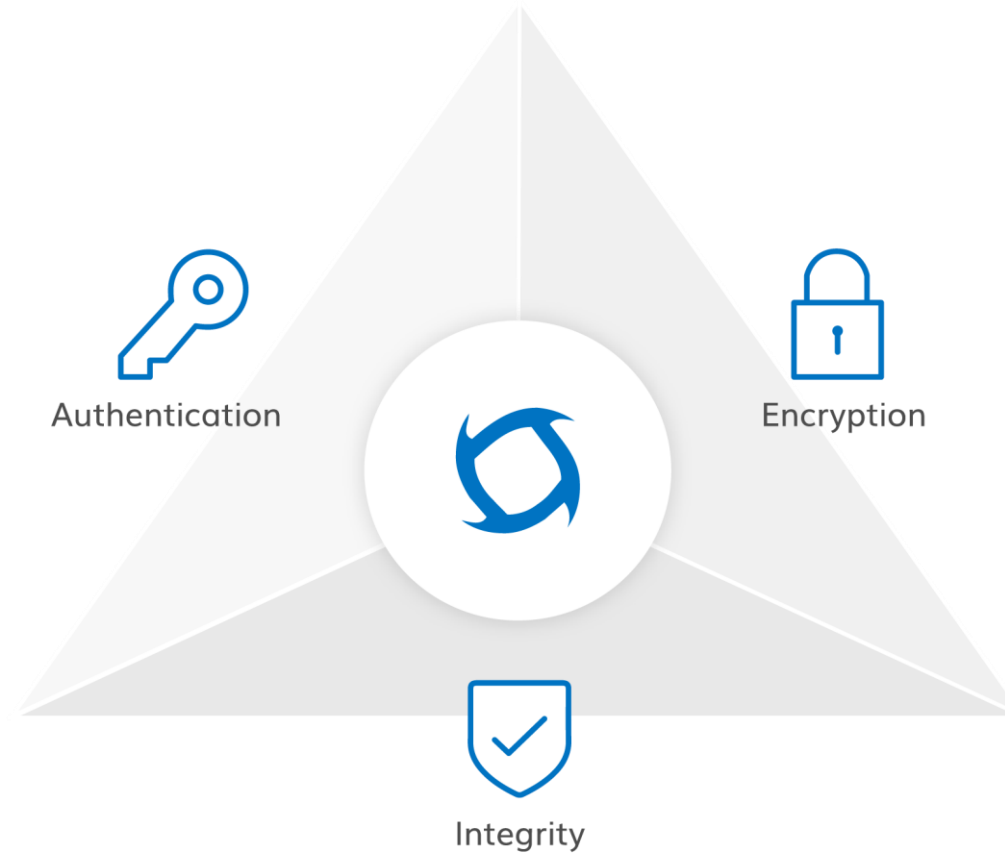
Never run unsigned code

Never trust unsigned data

Always Encrypt sensitive data



Cornerstones of Public Key Infrastructure (PKI):



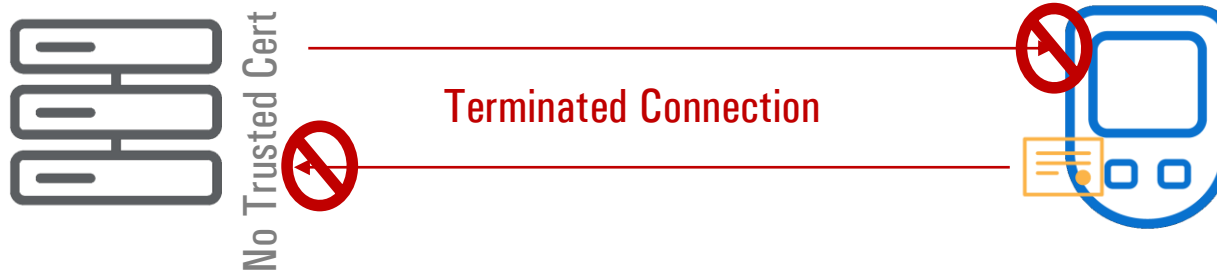
PKI is a **comprehensive framework** that contains the **set of roles, policies, and procedures** needed to manage, distribute, create, store, use and revoke **digital certificates**.

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)



01100
10110
11110



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



Thank you

Mike Nelson

VP of IoT Security

Mike.Nelson@digicert.com

 @mike_k_nelson