InformationWeek DARKReading

Preparing A Next-Generation IT Security Strategy

Sponsored by:

LogRhythm®

The Security Intelligence Company

UBM

Logistics

Optimize your experience today

- **Enable pop-ups** within your browser
- **Turn on your system's sound** to hear the streaming presentation
- **Questions?** Submit them to the presenters at anytime on the console
- **Technical problems**? Click "Help" or submit a question for assistance

UBM

LogRhythm
The Security Intelligence Company

InformationWeek DARKReading

Featured Keynote

Preparing A Next-Generation IT Security Strategy

Moderator

Tim Wilson
Editor in Chief
Dark Reading

Guest Speaker

Christie Terrill
Managing Director
Bishop Fox

UBM

InformationWeek DARKReading

Agenda

PREPARING A NEXT GENERATION IT SECURITY STRATEGY

- About Me
- Security Drivers
- Guiding Principles
- Traditional vs. Next Generation Approach
- Your Next Generation IT Security Strategy

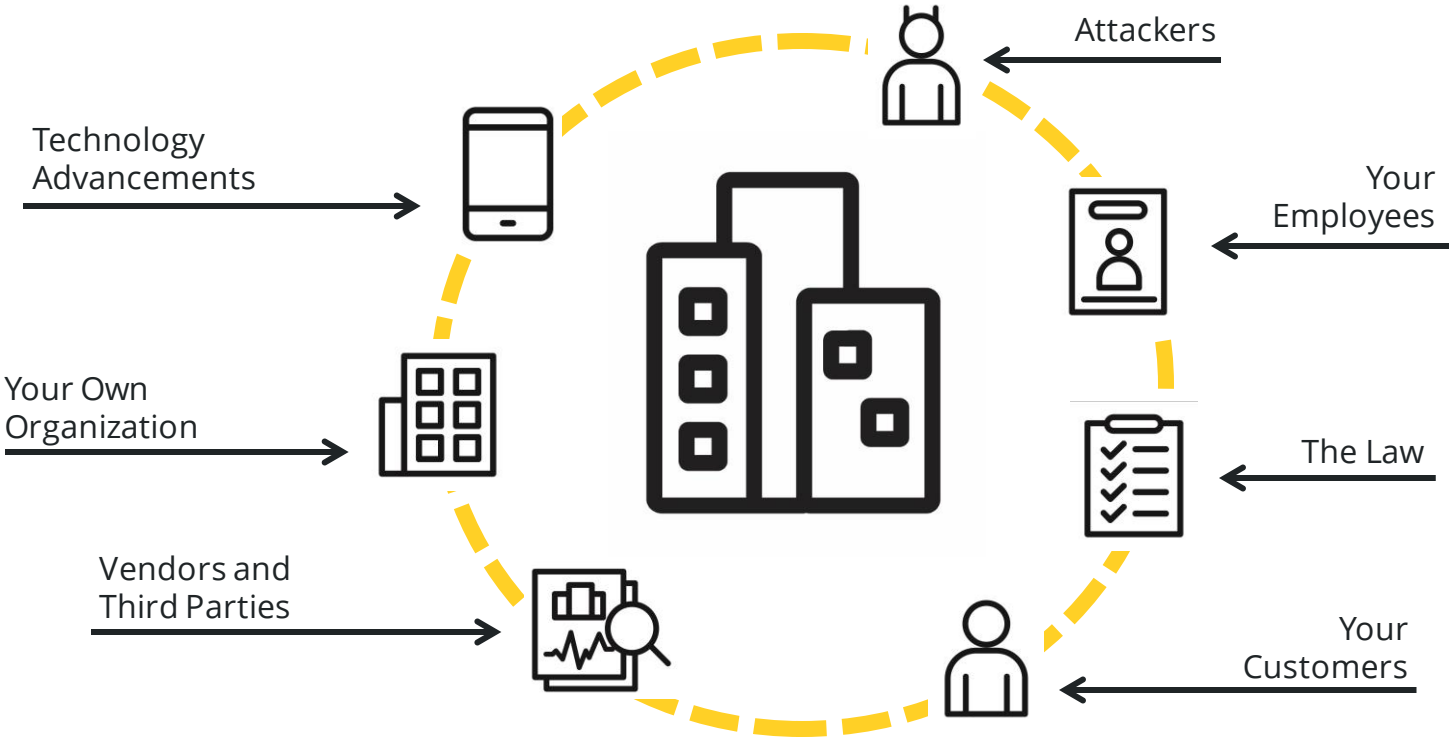
About Me

CHRISTIE TERRILL, PARTNER AT BISHOP FOX

- 15 years in global cybersecurity consulting for Fortune 500 and high-tech startups
- Focus on projects that impact the breadth of security and how it supports the business
- Pragmatic, not paranoid

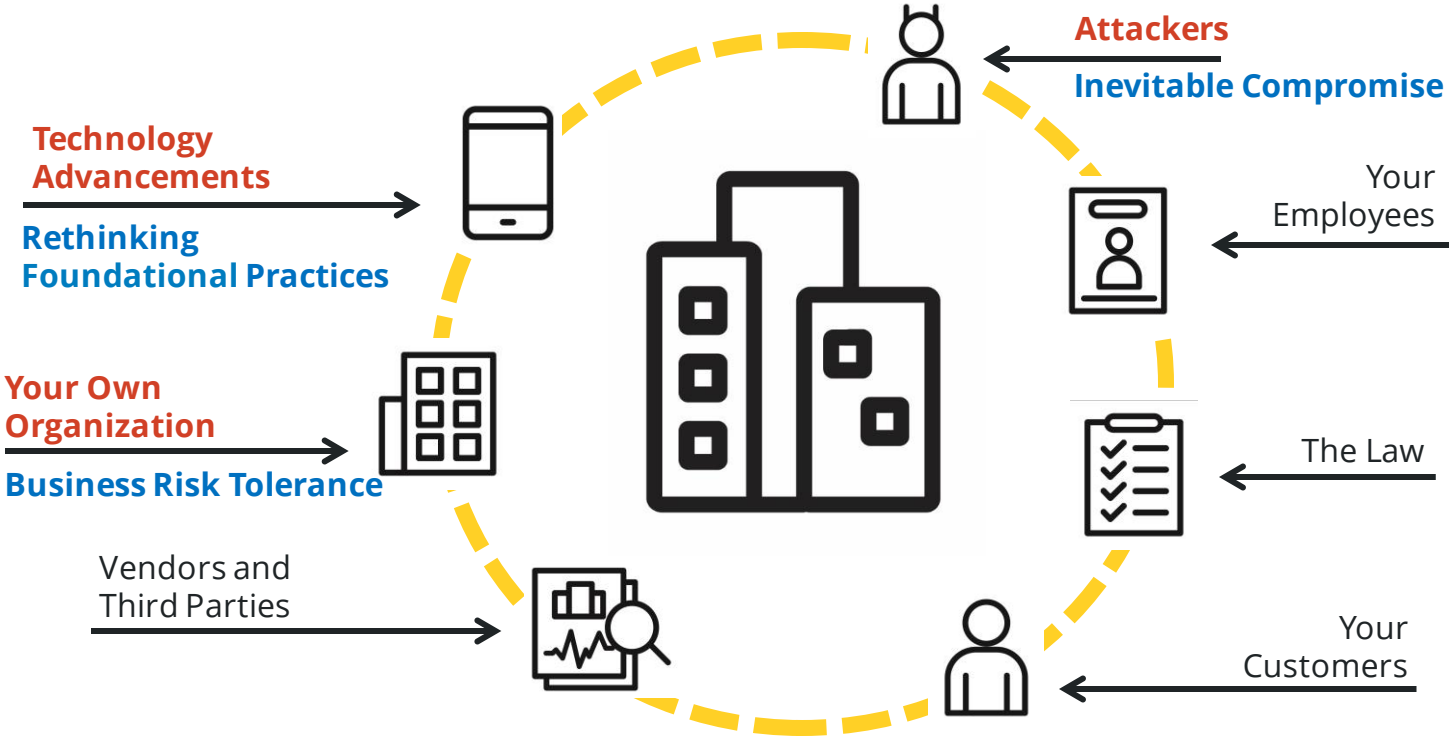
Security Drivers

WHAT KEEPS YOU UP AT NIGHT?



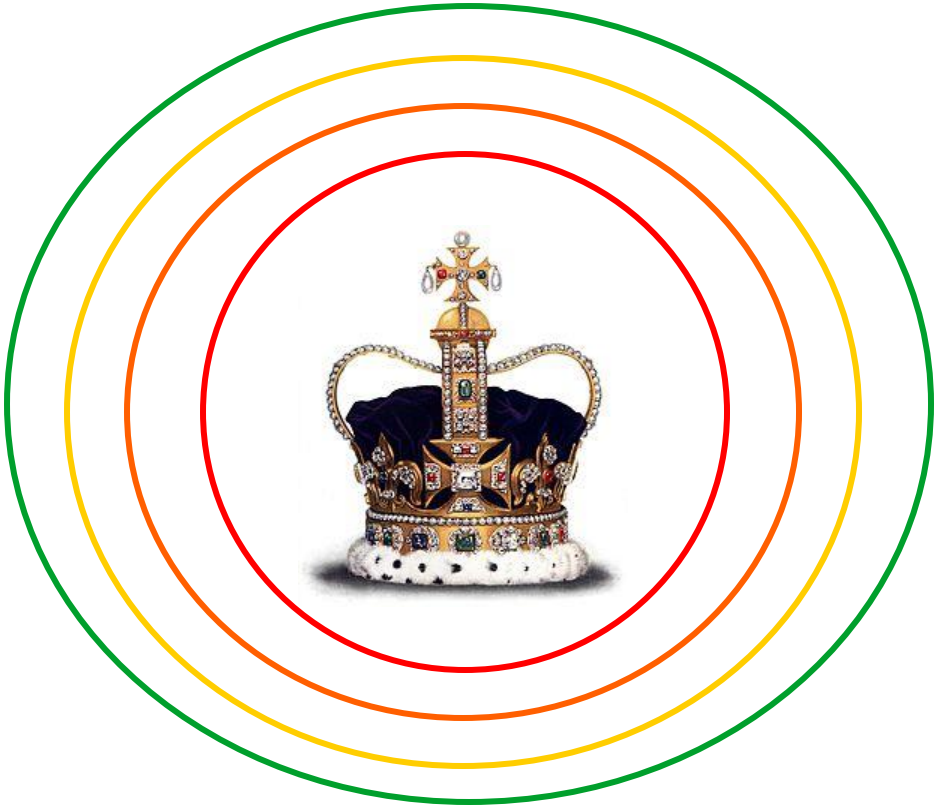
Guiding Principles

SECURITY STRATEGY ASSUMPTIONS



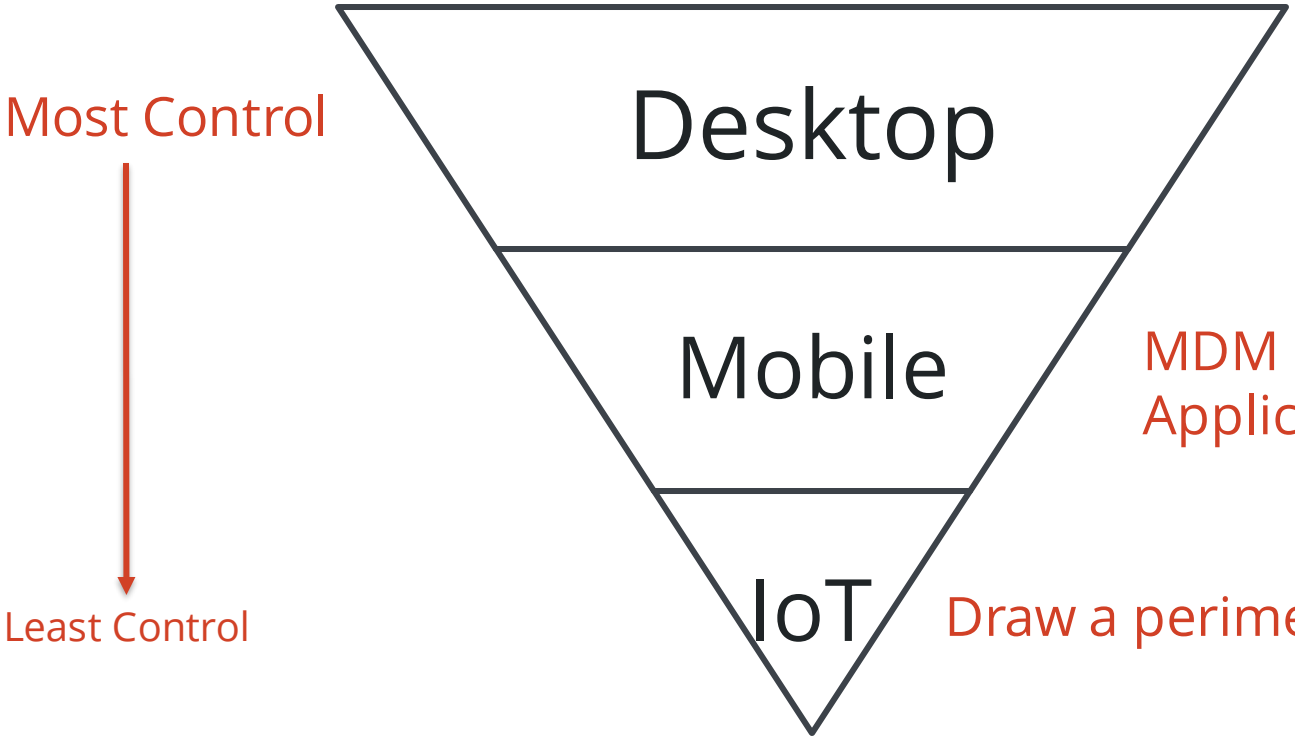
Traditional Approach

DEFENSE IN DEPTH AROUND THE CROWN JEWELS



Trending Now

LESS AND LESS CONTROL



Next Generation Approach

INTEGRATED PERSPECTIVE

Capabilities

WHAT CAN I ENFORCE?

Two different approaches work together symbiotically to enforce your security objectives

More Control

Control what options the node has via:

- Baseline configurations
- Agents (e.g. Antivirus)
- Local firewalls

Less Control

Control what the node talks to via:

- Secure access gateways
- Blackhole traffic
- API configuration

Context

WHAT WAS THE INTENT?

A more informed answer to the intent of the user or device

More Control

- Ability to interrogate device and establish context (e.g. 2FA)
- More granular boundaries around trusted and managed devices

Less Control

- Observable behavior only (e.g. Netflow, AD logs, DNS)
- Can enforce connectivity options based on device type (e.g. VPN for mobile)
- Larger perimeters around like devices

Challenge

WHAT CAN I LEARN AND ADAPT?

Continual feedback loop between red team and blue team to test your assumptions and close each discovered avenue for an attack

Red Team

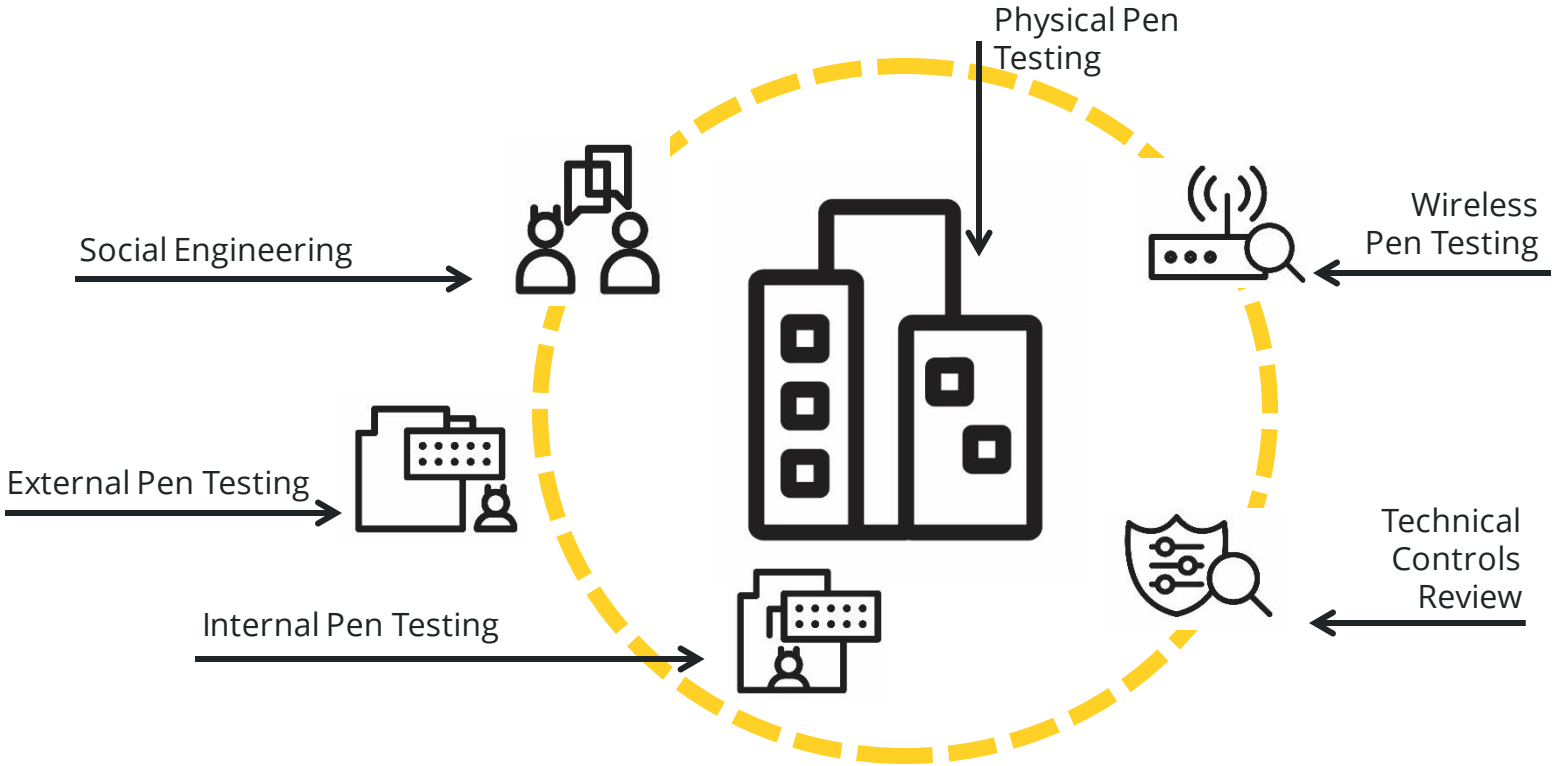
- Discover remaining attack vectors via simulations
- Conduct penetration tests and threat modeling
- Assist remediation efforts with expertise

Blue Team

- Improve on what was missed
- Constantly improve the data available to make good decisions
- Develop metrics to show improvement (or not) during simulations and real incidents

Challenge Yourself

RED TEAM OPTIONS

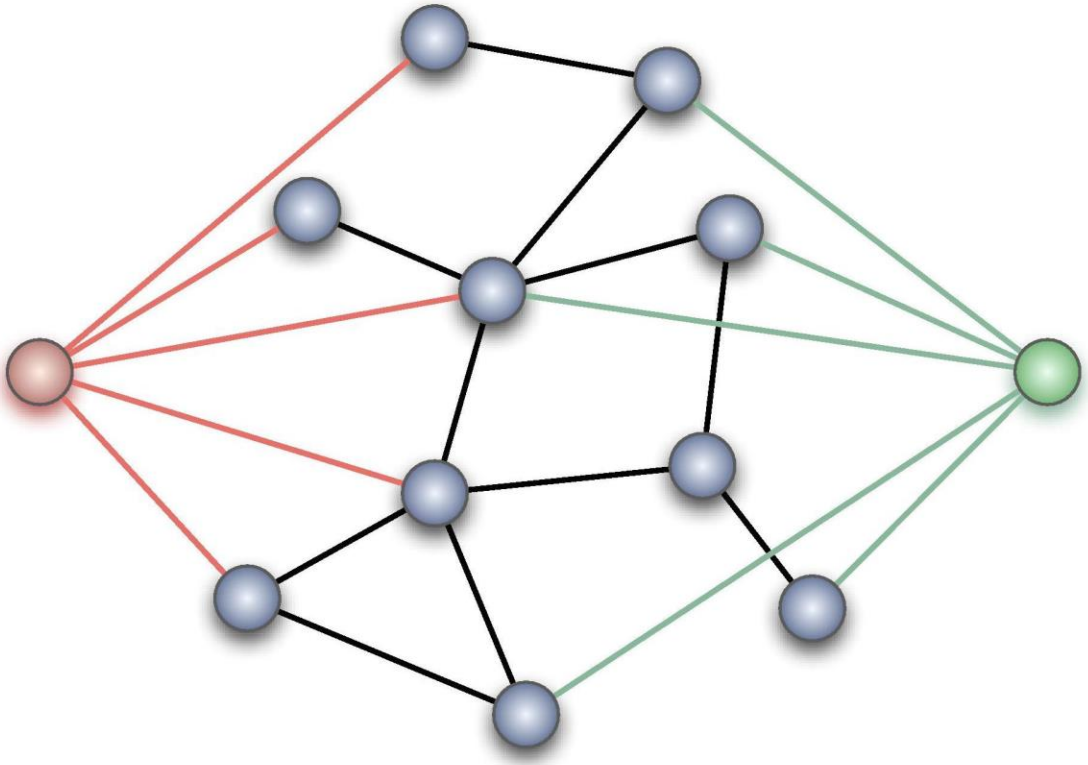


CONCLUSIONS

NEXT GENERATION IT SECURITY STRATEGY

Next Generation Strategy

INTEGRATED PERSPECTIVE



Commentary Desk

Preparing A Next-Generation IT Security Strategy

Moderator

Tim Wilson
Editor in Chief
Dark Reading

Commentator

Michael Dalgleish
Director, Sales Engineering
LogRhythm

UBM

LogRhythm
The Security Intelligence Company

InformationWeek DARKReading

Thank you for attending

Please visit our sponsor and any of the resources below:

- http://www.darkreading.com/events
- https://logrhythm.com/

InformationWeek DARKReading

LogRhythm
The Security Intelligence Company