SECURITY 101—
THE CRITICAL NEED TO GO BACK TO THE BASICS

Kate Kuehn
Vice President
Wandera
@KateKuehn
Security 101: Back to the Basics - Security Simplified

All people participating in the security ecosystem must understand one basic principle:

Risk + Cost = Security

What are the risks your organization faces & what is your role in the risk?

What is the “cost” when a breech happens? Opportunity & Capital

What is the true positive impact of understanding?
Security 101: A world of change

97%

48%

6:1

1000%
Security 101: Where to start?

Understanding the past is the key to a successful security future...

**Zone of routine**
Observable /Manageable

- What am expecting in a given year?

**Zone of surprise**
Uncertain / Insurable

- What incidents did we not plan for?

**Zone of catastrophes**
Rare/Extreme

- How can we learn from Infrequent but high impact events?
Security 101: The basic framework

**People**
- Make security everyone’s priority
- Continually review your assets and their related risks

**Process**
- Create and maintain the correct awareness and behaviours
- Make sure protection processes are automated
- Make sure that people know what to do when there is an incident
- Facilitate around-the-clock monitoring

**Technology**

**Identify**
- Understand what has happened, why, and LEARN from it

**Protect**
- Do the proper follow-up and analysis

**Detect**
- Make incident response and remediation a priority

**Respond**
- Ensure you have the practices in place to quickly safeguard your organization

**Recover**
- Make incident response and remediation a priority

**Identify**
- Understand what has happened, why, and LEARN from it

**Protect**
- Do the proper follow-up and analysis

**Detect**
- Make incident response and remediation a priority

**Respond**
- Ensure you have the practices in place to quickly safeguard your organization

**Recover**
- Make incident response and remediation a priority
Rule #1
Understand the real threat
Security 101: What are your biggest threats?

- Ransomware
- Distributed denial of service
- Trojans (banking or otherwise)
- CEO fraud or whaling
- Point of Sale frauds
- Personal data breach
- Espionage or IP theft
- Disruptive cyber attack

OR
Security 101: Employees as an “attack surface”

- 72% of employees use unauthorized file sharing for work.
- 1 in 7 users access gaming, adult or extreme sites weekly.
- 1 in 4 users access an insecure WiFi hotspot weekly.
- 27% of devices have an outdated OS.
- 1 in 25 apps leak sensitive credentials.

2. Inappropriate mobile activity – how serious is the problem? Research by Wandera August 2017
4. Mobile data report, Wandera July 2017
5. Mobile data report, Wandera January 2017
Security 101: How are they getting in?

- Capture emails
- Extract data
- Steal username & password
- Turn on the microphone
- Turn on the camera
- Track device location
- Sabotage device settings
- Capture emails
- Steal username & password
Rule #2
Everyone has a role to play to achieve great security...
Security 101: Where do your people have power?

Management

- How exactly is our organization’s data used?
- How do I reduce the risk of uncontrolled security costs?

Policy

- How can I enforce acceptable use policies on Wi-Fi?
- How do I make Compliance Policies effective 24/7?

Acceptable Use

- What is the usage breakdown of business vs. personal on assets?
- How can I better understand the risk of Shadow IT?

How do I block access to risky, unofficial applications?

How do I protect my users?

Content Security to protect data

- How do I protect my data?
Security 101: The Impact of Ignorance?

Top Cause of Data Breaches

- Attackers: 46
- Accidentally Made Public: 22
- Theft or Loss of Hardware: 21
- Insider Theft: 10
Rule #3:
Clouds can’t be cloudy..
Technology can’t be
Security 101: Complete data visibility

Employees

Data, apps & activity

Network and WiFi

Enterprise
Security 101: Stop threats before they arrive

Real-time blocks and alerts

Clean, compliant traffic

Full visibility and reporting
Security 101: What is our endgame?

1. Review and Implement a basic framework that focuses on the **zone of routine**

2. Good data security is something **EVERYONE** plays a part in. **INCLUSION & EDUCATION** are key.

3. Constantly review what data is **CRITICAL**, the **COLABORATE** on how to protect it, and **TEST** frequently your processes and the technology used to **SUPPORT** it.
THANK YOU

CONTACT INFO:
KATE KUEHN
TWITTER: @KATEKUEHN
EMAIL: KATE.KUEHN@WANDERA.COM