NEW DIRECTIONS IN CYBERSECURITY

Andrew Scharlott, CISSP | CISM | MSCS

April 2019

AGENDA

1. Cybersecurity Fundamentals
2. Recent Breaches
3. Old Model of Cybersecurity
4. New Model of Cybersecurity
5. Current Challenges
6. Future Directions

CYBERSECURITY FUNDAMENTALS – THREATS & RISKS

- Cybersecurity is primarily about:

Assessing Threats & Managing Risk

CYBERSECURITY FUNDAMENTALS - CIA TRIAD

CYBERSECURITY FUNDAMENTALS - CIA TRIAD

- **Confidentiality**
  Access to information is only granted to those who need it

- **Integrity**
  Information is trustworthy and accurate

- **Availability**
  Information is accessible when needed

RECENT BREACHES = VIOLATION OF “CIA”

AdultFriendFinder

Marriott

Anthem

YAHOO!

T.J.maxx

SONY

EQUIFAX

CYBERSECURITY: THE OLD “CASTLE” MODEL

- Historically, organizations viewed information security through the lens of the “castle” model
- The core idea is that the inside is “safe” - so we just needed to keep the bad guys out

This has proven repeatedly to not be valid

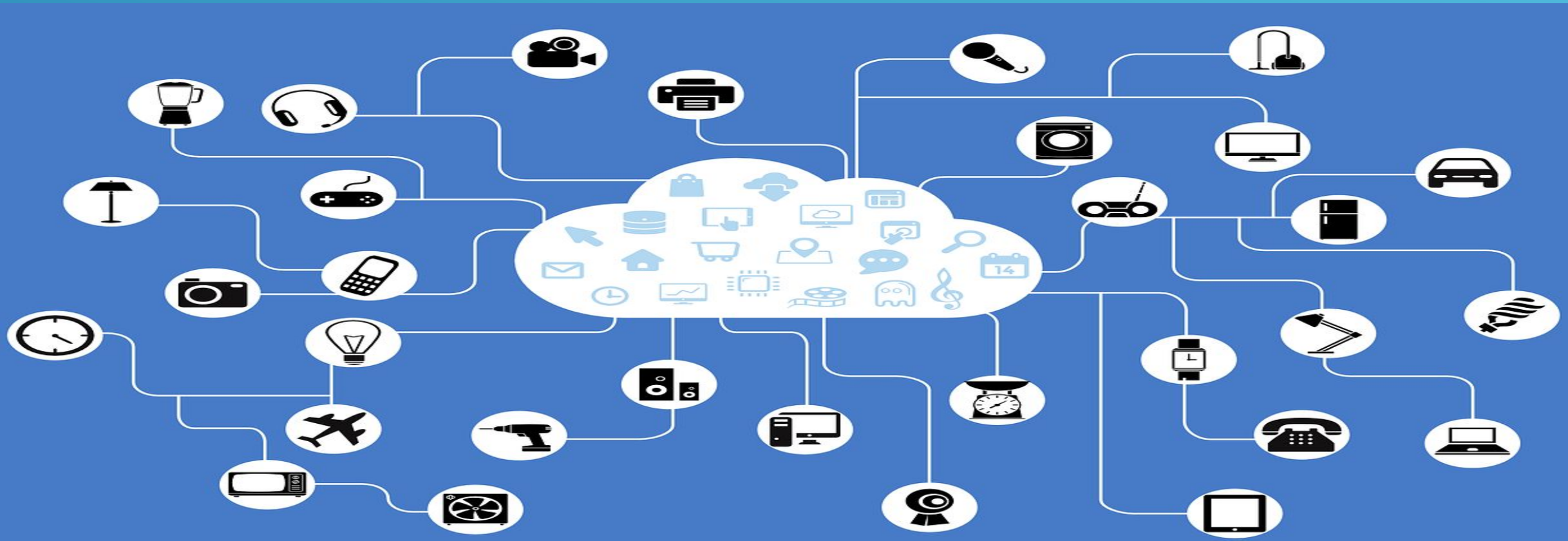
CYBERSECURITY: THE NEW MODEL

- Now we assume our networks are compromised

- This means the task at hand is to identify and contain the bad actors as much as possible

CYBERSECURITY: CHALLENGES

- Explosive growth in dependence on technology
- More users and devices online (IOT)
  - *will be an estimated 50 billion devices online by 2020*

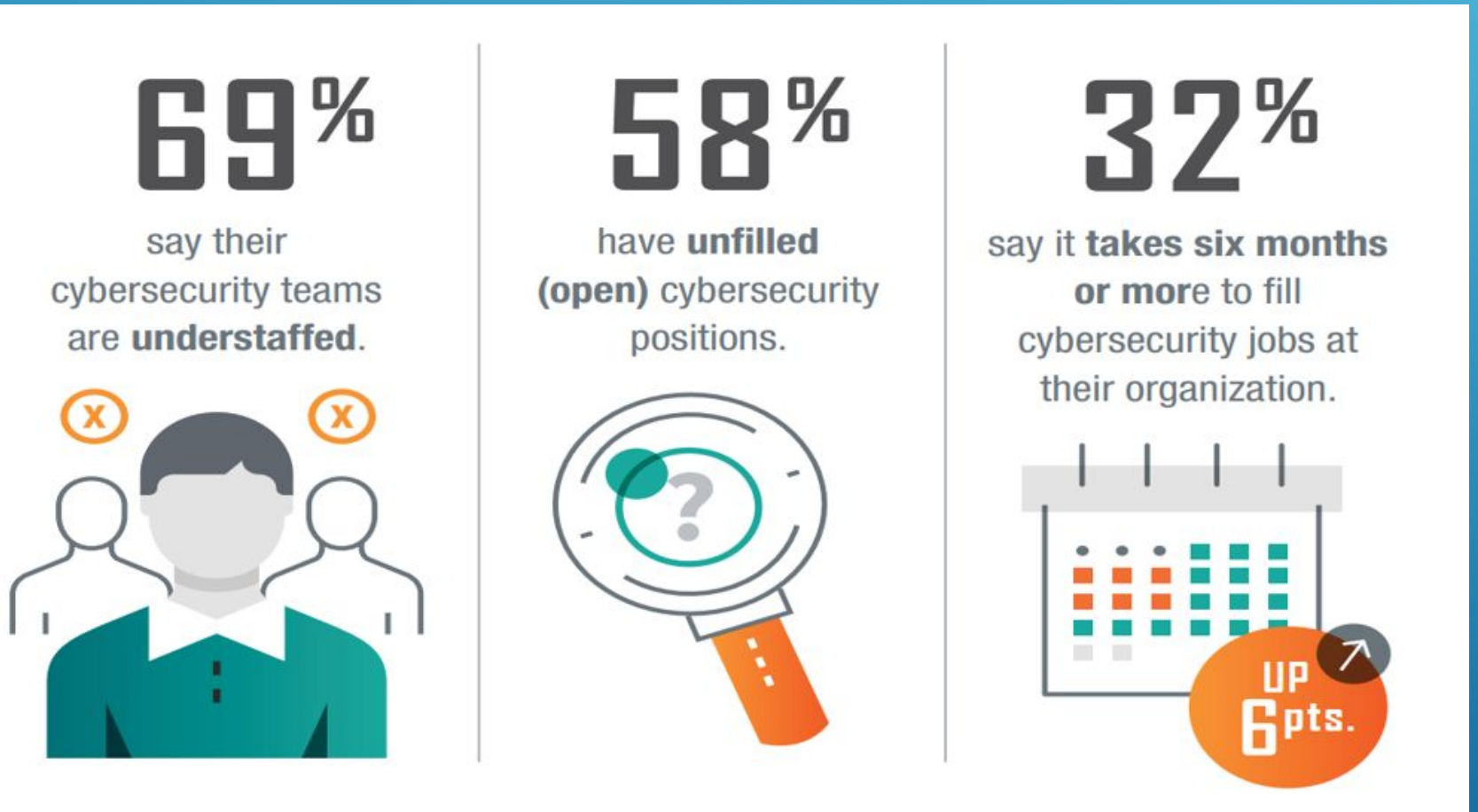


CYBERSECURITY: CHALLENGES

- Attackers are more sophisticated, aggressive, and better funded
  - State actors
  - Organized crime

CYBERSECURITY: CHALLENGES

- Massive shortage of skilled Security professionals
  - Per $(ISC)^2$, there will be over 1.5 million *unfilled* cybersecurity positions by 2020



CYBERSECURITY: WHAT'S NEXT

Where are we going?

What are our upcoming challenges?

What are our upcoming opportunities?

1. COMPLIANCE, PRIVACY, AND OTHER REGULATIONS

- GDPR, CCPA, and other privacy laws/regulations coming into effect
- Increased focus on user-controlled data (e.g. Facebook)
- Increased hiring and certification of Privacy-focused professionals

1. COMPLIANCE, PRIVACY, AND OTHER REGULATIONS

“ effective privacy and data protection needs a globally harmonized framework ”

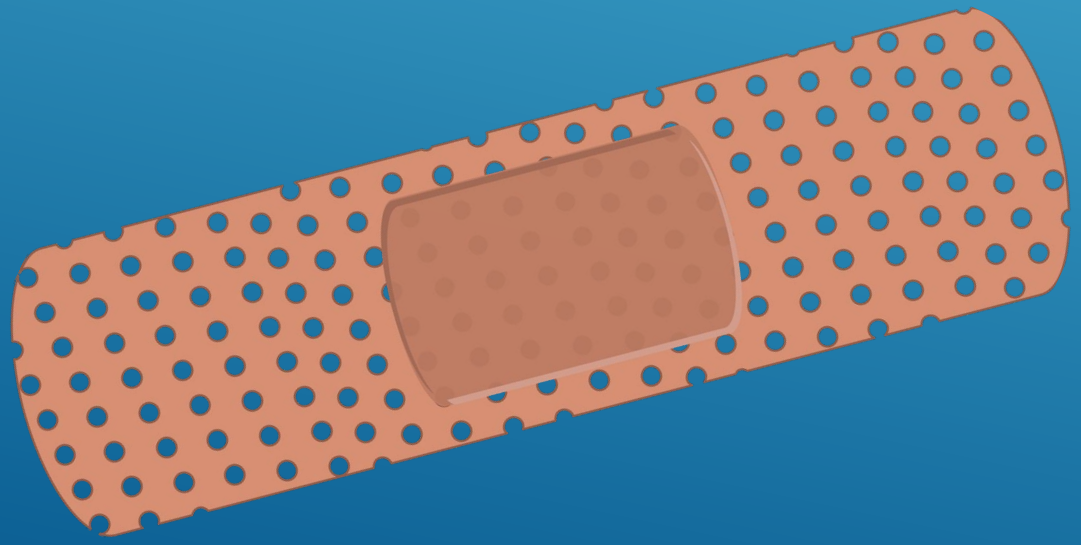
- Mark Zuckerberg (*Washington Post* op-ed)

1. COMPLIANCE, PRIVACY, AND OTHER REGULATIONS

One important note…

Compliance is not Security

Compliance is "***basic security hygiene***"



2. THREAT HUNTING AND BREACH CONTAINMENT

- Our current/new assumption is that we are compromised
- We need to (re)focus on finding the problem and containing the incident

Per IBM: "On average, companies take about 197 days to identify and 69 days to contain a breach“

3. DATA PROTECTION (NOT NETWORK PROTECTION)

- We've seen that it is (practically) futile to try to keep the bad guys out of the network

- We need to focus on protecting the really valuable data to our organization
  - Trade secrets
  - Customer data
  - PII / PHI
  - Engineering specs
  - Etc.

- Move protective mechanisms closer to where the data is actually stored

4. ADVANCED DEFENSE & DETECTION TECHNIQUES

- We need to move beyond simple (or even advanced) signature detection tools
  Traditional Anti-Virus misses a lot

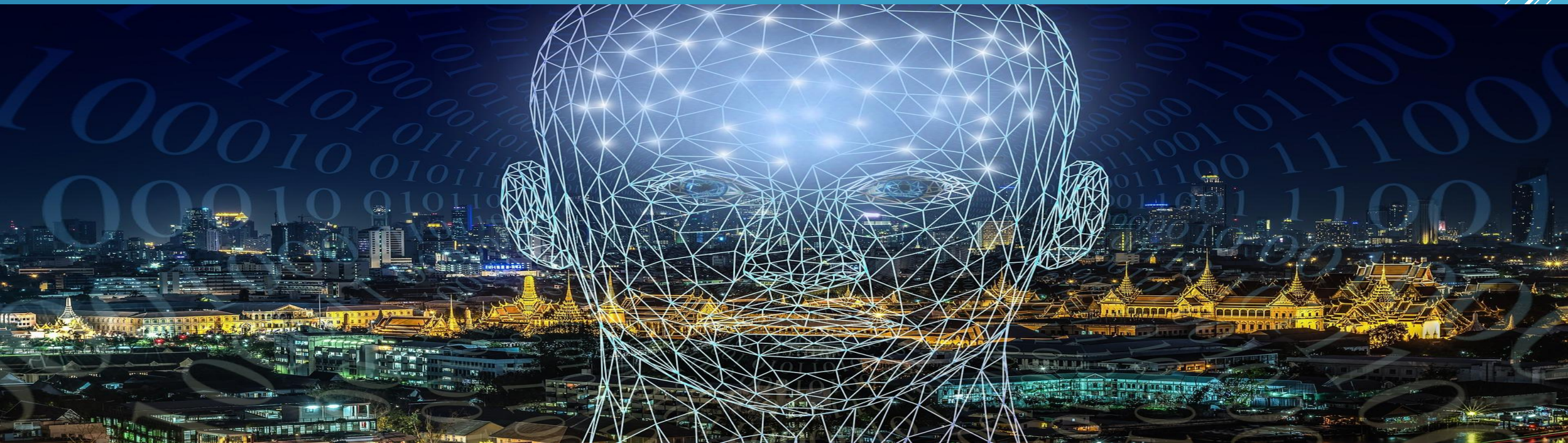
- New areas of focus
  - User Behavior Analysis (UBA) & Pattern Detection
  - Artificial Intelligence

- We need to be aware of *Alert Fatigue*
  - Advanced Technology is essential to fight against this

4. ADVANCED DEFENSE & DETECTION TECHNIQUES

- User Behavior Analytics (UBA)
  - Focuses on patterns of behavior
  - Can identify something out of the ordinary

- A.I. and other advanced techniques are being used by the bad guys; we need similar capability/speed in defense too



5. SUPPLY CHAIN SECURITY – "ISLAND HOPPING"

- Even if we do a perfect job with our own networks/users, we still have a wide-range of business partners that may have access into our networks and computer systems

- If your business partner gets compromised and they have access to your network and data systems… you have a problem too

"Island Hopping" (aka "Leapfrogging"): "*attackers go after their target's affiliates first – preferably smaller companies who may not be as protected… then use these companies to gain access … to the target company*" (TrendMicro)

6. ZERO TRUST NETWORKS (ZTN)

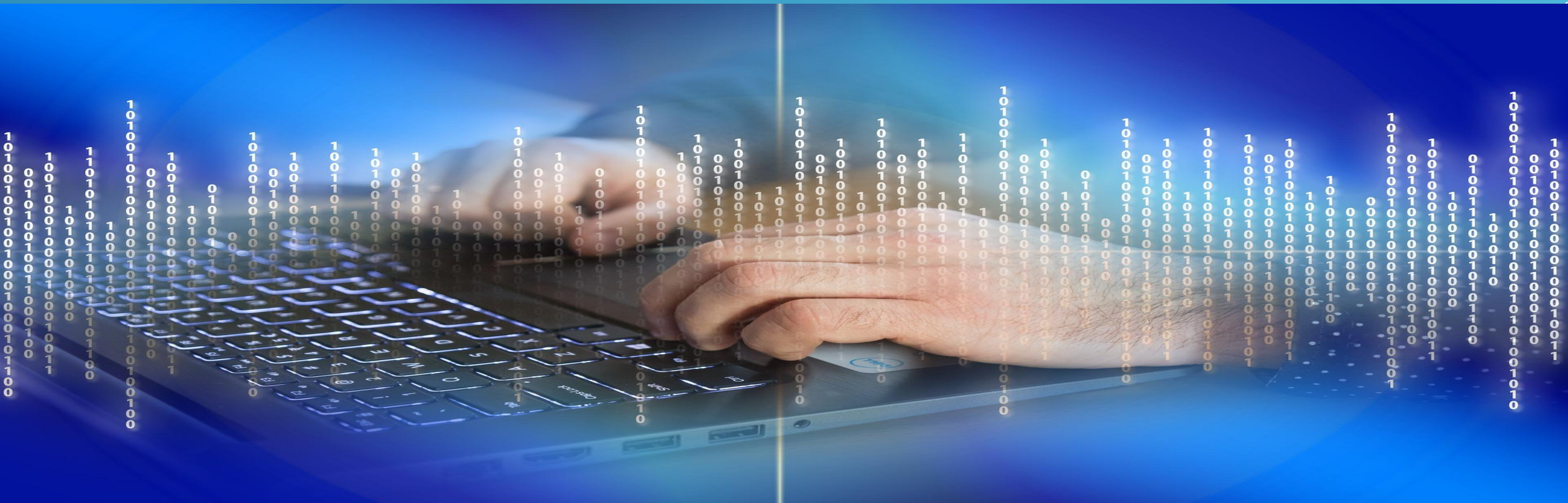
- Focus on authorizing the action/request, rather than the device/user

- Goes beyond just checking authentication – tries to get to whether the specific *action* is allowed

Note: the technology available to actually implement this at large enterprise scale is still a few years away

7. ACCOUNT MANAGEMENT & AUTHENTICATION

- Privileged Account Management (PAM)
  - Focus on your most critical accounts / users with a lot of access (e.g. Domain Administrators, DBAs, etc.)
  - Can apply extra requirements (e.g. biometrics, PIN, etc.) and enable enhanced monitoring and logging



7. ACCOUNT MANAGEMENT & AUTHENTICATION

The average business employee must keep track of 191 passwords… 81% of confirmed data breaches are due to passwords (report from LastPass)

7. ACCOUNT MANAGEMENT & AUTHENTICATION

Highly complex and secure passwords are good…
… but having no passwords is even better

- Multi-factor Authentication (MFA) examples:
  - Smartcard + PIN
  - Password + Cell Phone Code (e.g. *Duo*, *Google Authenticator, etc.)*
  - Fingerprint + Password

8. ATTACKS INCREASINGLY IMPACT THE PHYSICAL WORLD

- Historically, attacks have mostly been confined to the digital world

- Recent attacks/trends show move to physical manifestations as well:
  - Stuxnet, Triton malware, & HVAC/ICS attacks
  - Ransomware impacts (NIH)
  - Medical devices

9. CLOUD ADOPTION & EXPANSION

- In 15 months, 80% of all IT budgets will be committed to cloud solutions
- 73% of companies are planning to move to a fully software-defined data center within 2 years
- 96% of respondents now use cloud

From:
Intel (2017)
RightScale (2018)

9. CLOUD ADOPTION & EXPANSION

- Security Concerns Around Cloud:
  - Just 23% of organizations today completely trust public clouds to keep their data secure
  - **49% of businesses are delaying cloud deployment due to a cybersecurity skills gap**

From:
Intel (2017)
RightScale (2018)

NEW FOCUS AREAS - IN CONCLUSION

1. Compliance, Privacy, And Other Regulations
2. Threat Hunting And Breach Containment
3. Data Protection (Not Network Protection)
4. Advanced Defense & Detection Techniques
5. Supply Chain Security – “Island Hopping”
6. Zero Trust Networks (ZTN)
7. Account Management & Authentication
8. Attacks Increasingly Impact The Physical World
9. Cloud Adoption & Expansion