

SECURITY THAT MAKES A DIFFERENCE

Overview of the 20 Critical Controls

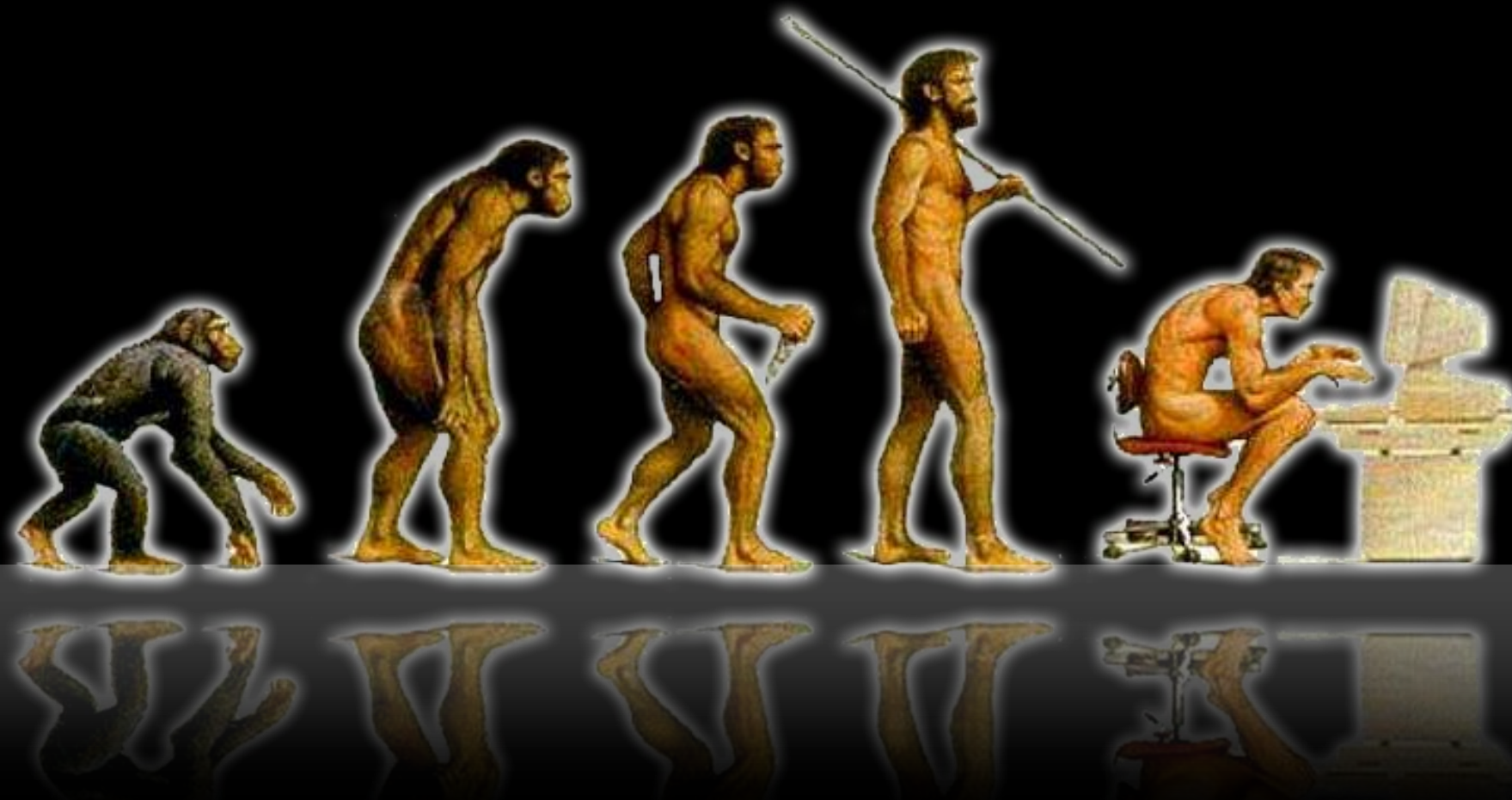


Dr. Eric Cole

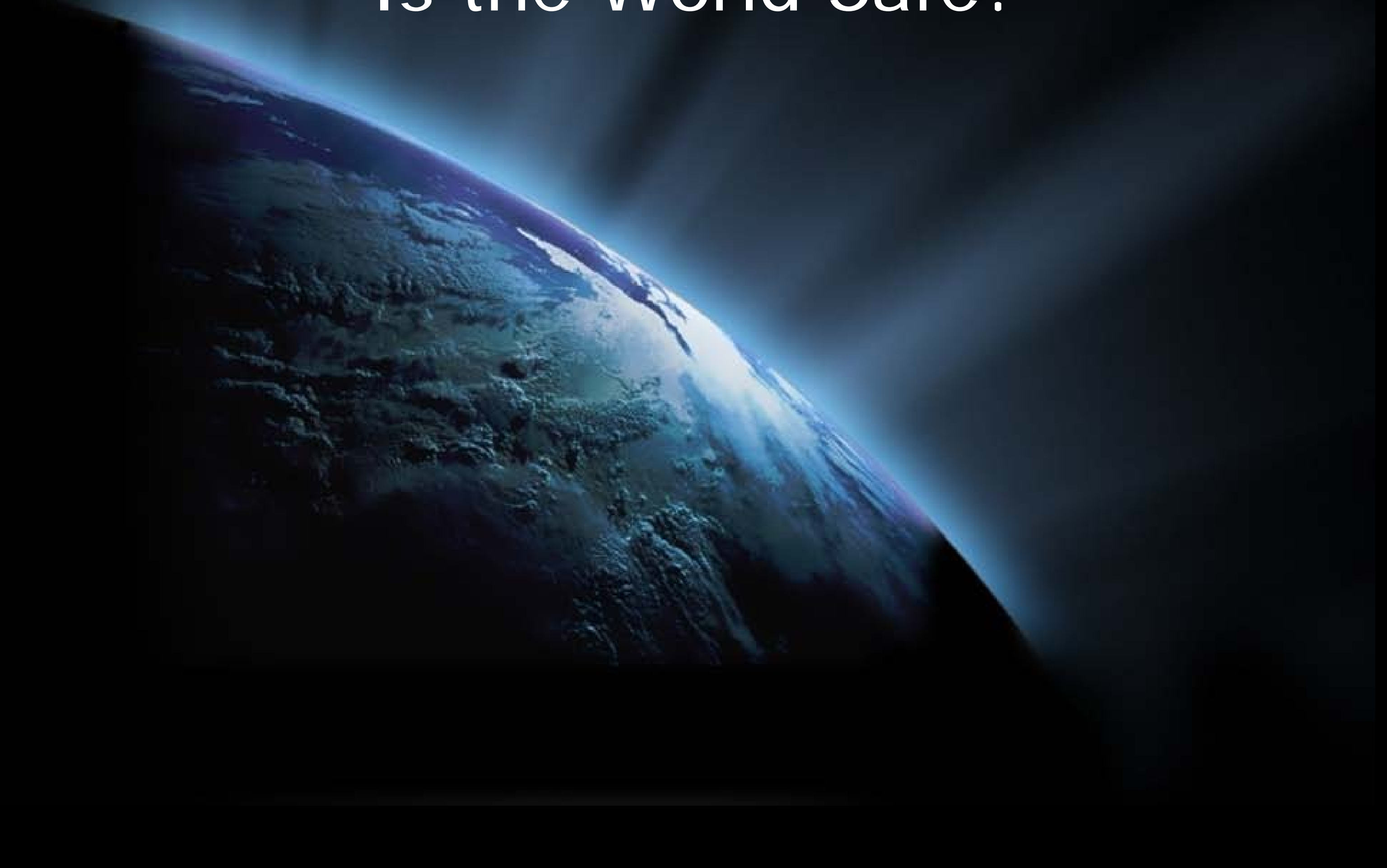


Introduction

- Security is an evolution!
- Understanding the benefit and know how to implement the 20 critical controls is key.
 - The controls are prescriptive
 - The controls can be automated



Is the World Safe?



Examples from the News

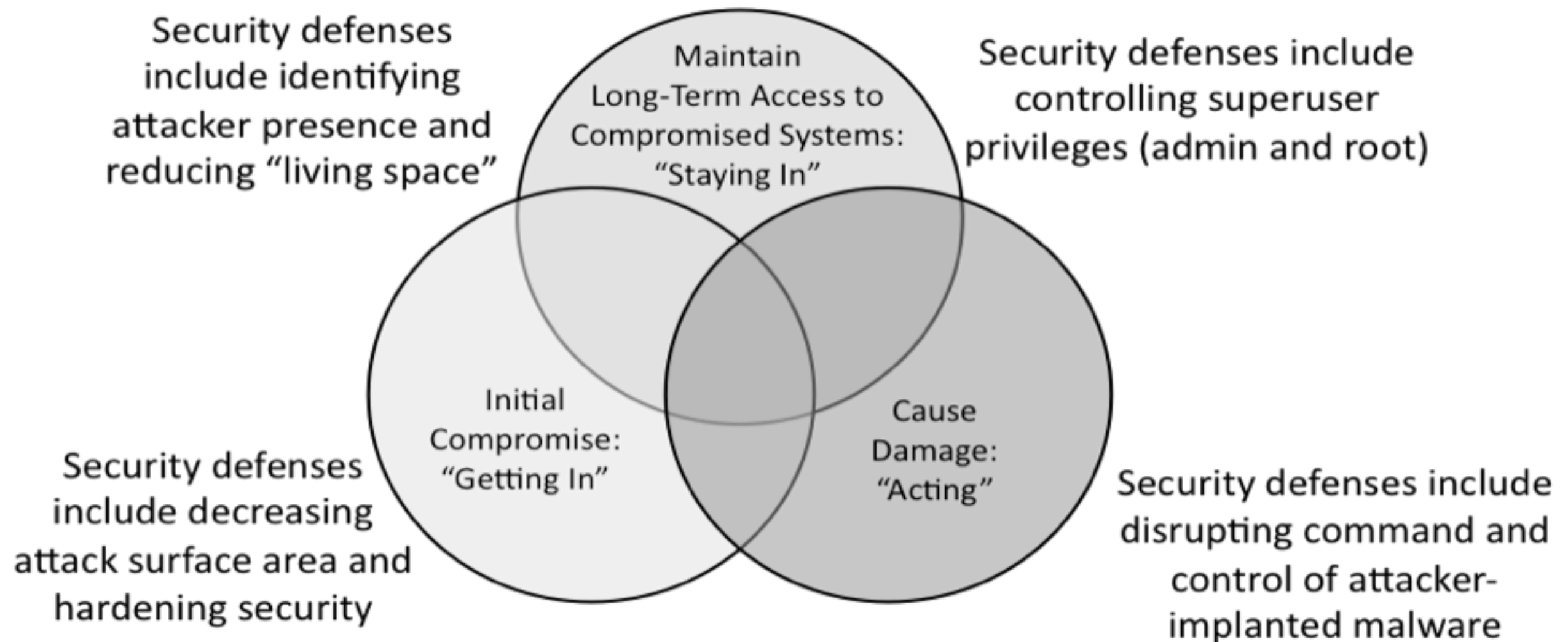
- PrivacyRights.org (updated weekly)
- Here are some that are reported (most are not)
- Just a small sample (organization/records breached):
 - Heartland Payment Systems (130+ million – 1/2009)
 - Oklahoma Dept of Human Services (1 million – 4/2009)
 - Oklahoma Housing Finance Agency (225,000 – 4/2009)
 - University of California (160,000 – 5/2009)
 - Network Solutions (573,000 – 7/2009)
 - U.S. Military Veterans Administration (76 million – 10/2009)
 - BlueCross BlueShield Assn. (187,000 – 10/2009)

Why is it Important?

- Government & private sector organizations are being attacked and compromised daily
- What we're doing today to defend systems is mostly not working!
- We are spending money defending against attacks that are not happening.
- We need priorities and a meta-view of the problem
- We need someone to take a stand and provide the industry with a set of real priorities for defense

Types of Computer Attacker Activities these Controls Are Designed to Help Thwart

Computer Attacker Activities and Associated Defenses



Project Guiding Principles

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Enterprise environments must ensure consistent controls across an enterprise to effectively negate attacks.



Categories of Sub-Controls

- Quick Wins (QW)
- Improved Visibility and Attribution (Vis/Attrib)
- Hardened Configuration and Improved Information Security Hygiene (Config/Hygiene)
- Advanced (Adv)



Why are the Controls Important?

- Cyber security is complex and becoming even more complicated every day
- Organizations are being compromised, even after spending large portions of their budget on infosec
- CIOs & CISOs need prioritized controls to get the most return from their investment
- More controls rarely hurt, but how do we decide which controls to start with?
- **It's critical that we have priorities!**

Critical Controls: 15 + 5

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software on laptops, workstations, and servers
4. Secure configurations for network devices such as firewalls, routers, and switches
5. Boundary Defense

Critical Controls (2 of 4)

6. Maintenance, Monitoring and Analysis of Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
10. Continuous Vulnerability Assessment and Remediation

Critical Controls (3 of 4)

11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Critical Controls (4 of 4)

16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training To Fill Gaps

Future Evolution of the Controls

- The controls are meant as a living document
- New updates come up periodically based on new threat and attack patterns
- While the document might change, the core controls represent a solid start and critical foundation to build a security program on
- The principles of the controls are sound and represent a clear path for automation and keeping pace or staying ahead of the threats

Critical Controls Summary

- Most organizations are not aware of what is happening on their network
- Many organizations do not have enough staff to tackle all of the difficult problems
- The critical controls provides a focused approach for automating and better understanding the areas that organizations need to focus on to increase their overall security.
- For more information on the CAG please reference: <http://www.sans.org/critical-security-controls/>

THANK YOU for your time

Dr. Eric Cole is an industry-recognized security expert with over 20 years of hands-on experience. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Cole has a master's degree in computer science from NYIT and a PhD from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting in which he provides state of the art security services and expert witness work. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS faculty fellow and course author.

Dr. Eric Cole



Twitter: [drericcole](#)
ecole@secureanchor.com
eric@sans.org