Zero Trust in Healthcare

Never trust, always verify

Stew Wolfe, CISSP, CISM, CISA

NTT Canadian Cybersecurity Practice lead

Zero Trust in Healthcare

- Healthcare is being driven by digital innovation. However, with the vast expansion of the landscape, the number of attack vectors have increased in tandem
- Security teams want to enable physicians to access patient data anytime from anywhere in a secure, unobtrusive way
- Healthcare is the leading industry suffering from insider threats today. Inside actors are involved in 58% of security breaches

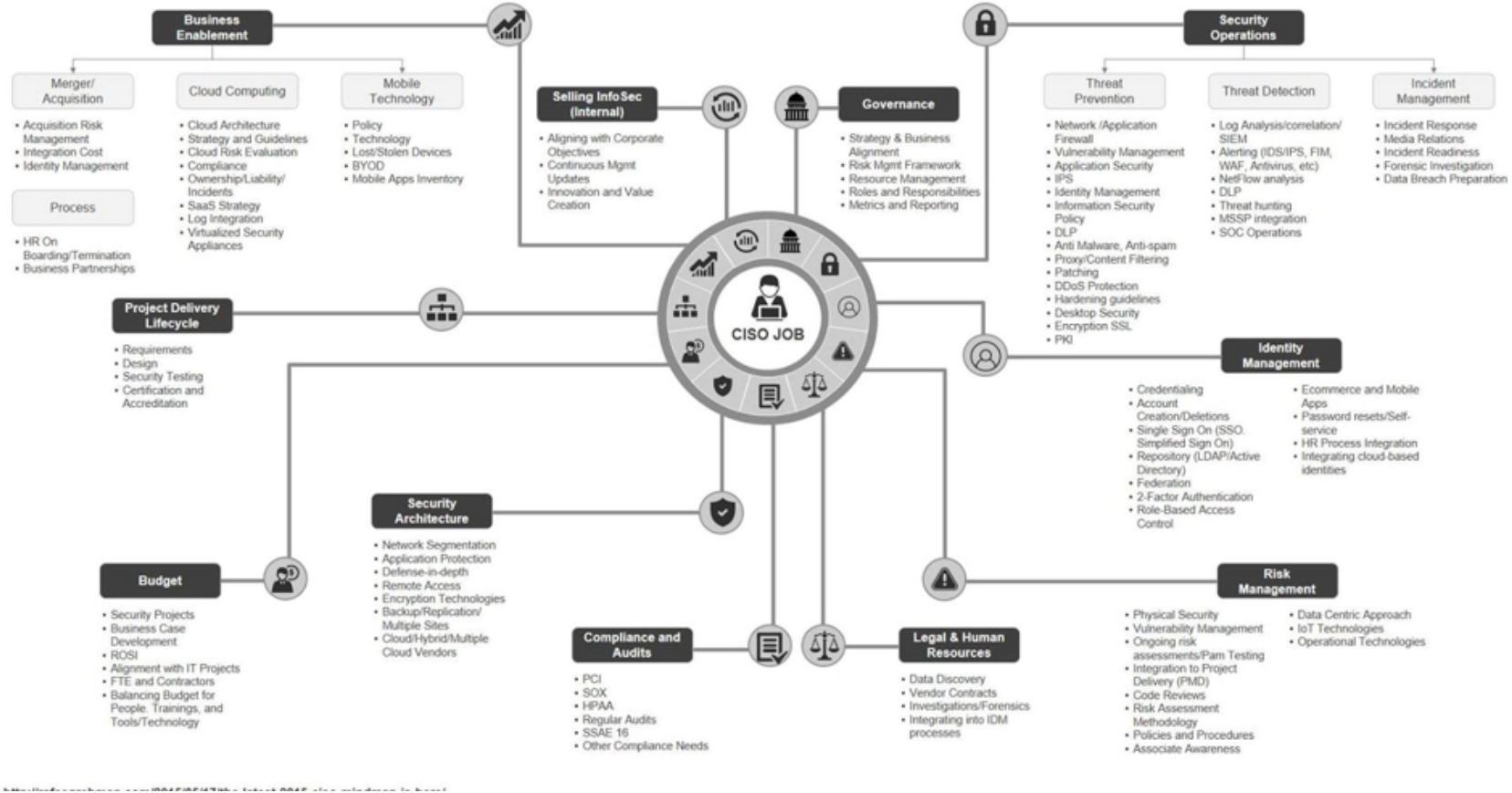
- Confidential patient information including diagnosis, treatment, history, and payment records sell for a pretty penny on the Dark Web, sometimes at a rate as high as $1,000 per record.

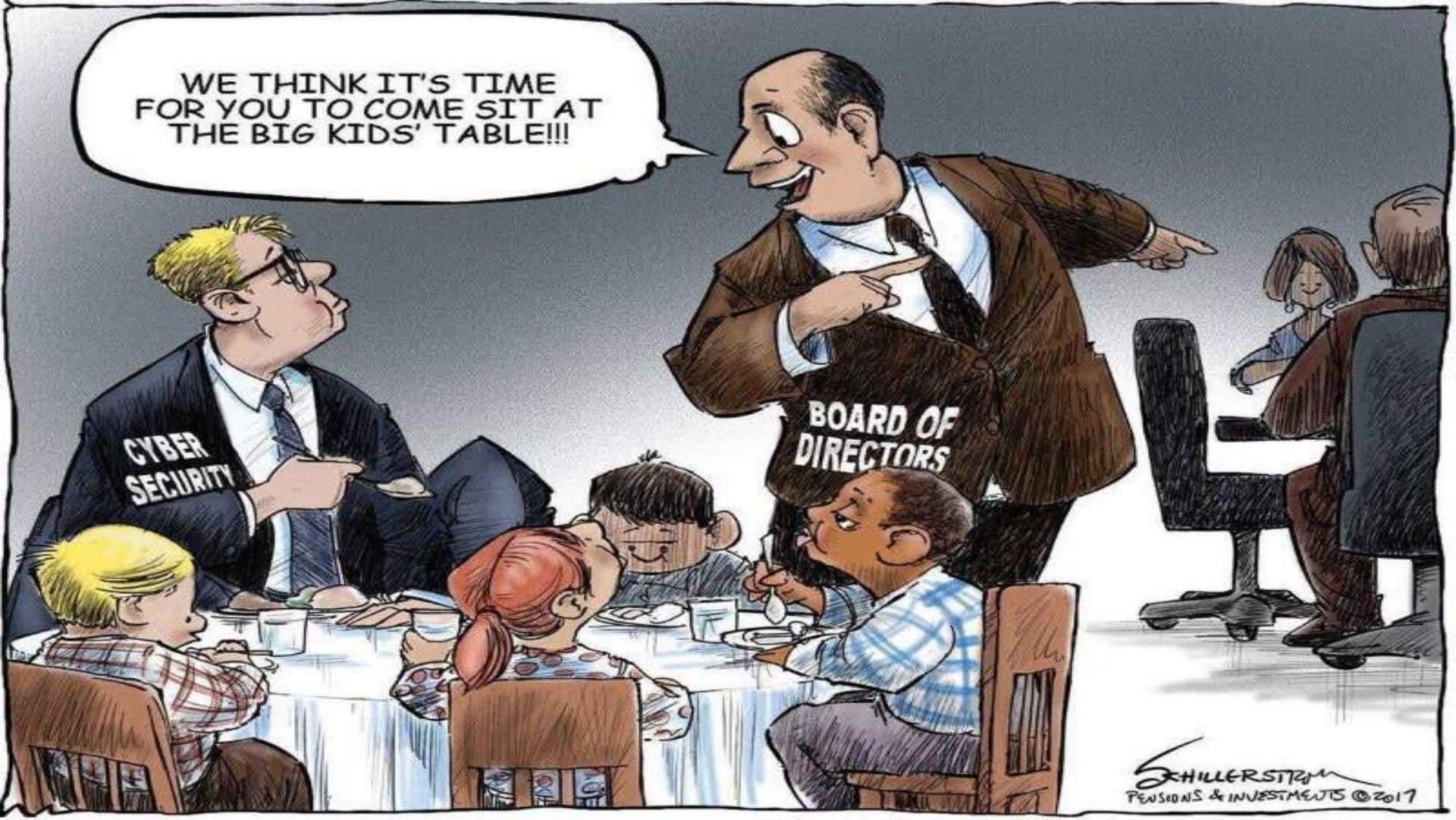
Zero Trust in Healthcare

- Patient-driven care - trust those caring for them to safeguard their data
- Access must be secure to EHR and accountable, regardless of whether the data resides especially with BYOD
- The network must have strong security measures, such as physical segmentation and firewalls - Secure by Design
- Ensure that all patient data and resources are accessed securely with the appropriate permissions

- Have in place a “least access” strategy and grant access only to people authorized to access data

Security by Design – *The CISO challenge*

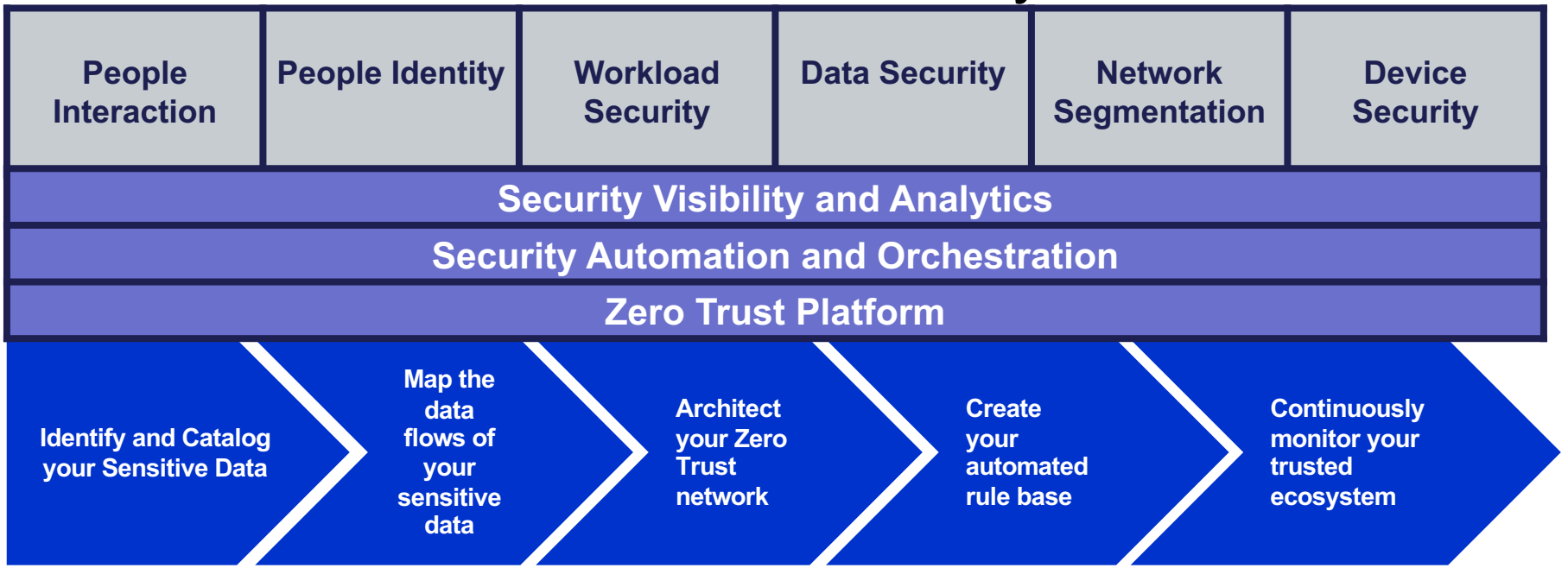



WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS ©2017

Five Guiding Principles of Measuring Zero Trust

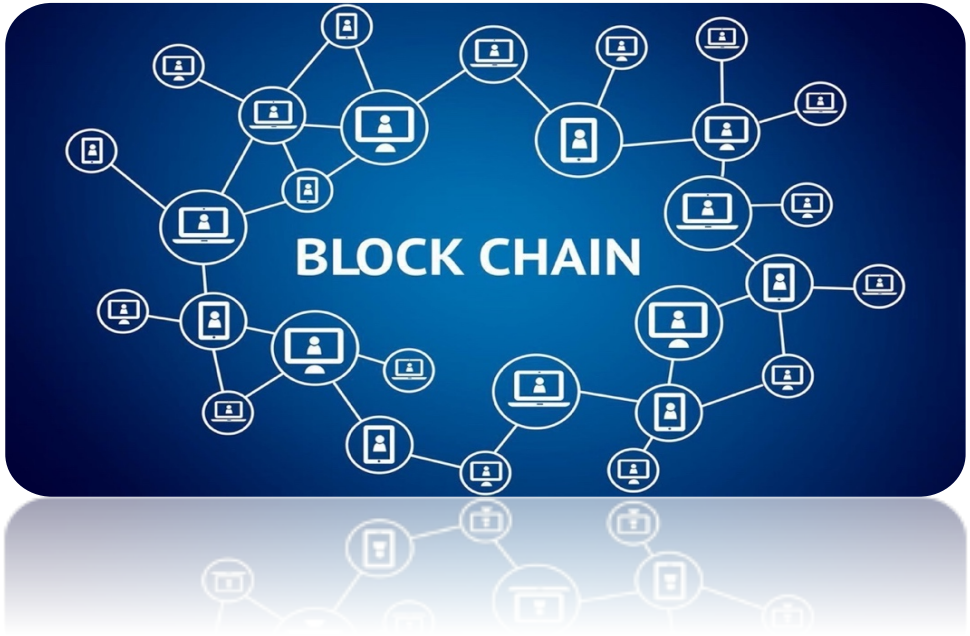
Zero Trust Networks by Evan Gilman and Doug Barth O'Reilly Media 2017

Nine Pillars Of The Zero Trust Ecosystem



Zero Trust in Healthcare

- Zero Trust has three pillars: 1) verify every user's identity, 2) authenticate every device, and 3) limit privilege and access to data
- It helps to secure the network by shrinking the security perimeter and preventing unchecked and unrestricted movement by an attacker within the network
- Authenticating devices and users is par for the course in the Zero Trust conversation.
- But it's not always just access to data by an unauthorized or malicious individual that causes disruption. The other half of the equation is ensuring the data itself is authentic through the use of Blockchain



"WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

Zero Trust in Healthcare

- Many healthcare organizations still run legacy components in their digital operations which enable ‘easy pickings’ for an attacker
- Doctors especially are demanding of having the freedom to access the network regardless of where they are
- Traditionally healthcare organizations such as hospitals typically have flat organizational structures and networks. The side effect is that this makes lateral movement by attackers significantly more of a guarantee

- It takes healthcare organizations an average of 402 days before discovering a breach has occurred.

Security Silos Complicate Protection

- Most healthcare institutions have between 45 and 65 security vendors
- Most vendor systems don’t talk to each other!

Zero Trust in Healthcare

- The core principle of Zero Trust is to “never trust, always verify.”
- All resources must be accessed in a secure manner, regardless of location
- Access control is on a need-to-know basis and is strictly enforced
- Organizations must inspect and log all traffic to verify users are doing the right thing
- Focus on not just authenticating and authorizing access at the front gate, but continuously throughout the user’s experience

- It’s no longer about the network—it’s about the people who access your systems, and the access controls for those individuals.

Drivers for Healthcare

The number of days to recover from a breach on average is

up 9 days

vs last year*

*2019 NTT Security Risk Value Report

Zero Trust in Healthcare

- Context-based access policies - user's context (Who are they? Are they in a risky user group?), application context (which application the user is trying to access), device context, location and network

- We need to set allow the risk scoring based on those contextual signals to determine the riskiness of a particular authentication event, and prompt for a second factor based on that insight

- Trust is also no longer absolute: this adaptive authentication is continuously monitored for a change in one of those signals

AND IN THE NEWS…

- Only device manufacturers are permitted to apply for an investigational testing authorization involving medical devices
- Proposed changes will allow independent researchers and health care professionals to file an application for investigational testing
- Health Canada will also require hospitals to report security incidents
- Health Canada is also developing a framework to expand the use of real-world evidence to monitor the safety and effectiveness of devices post-market