Core Principals of Cyber Hygiene

In a World of Cloud and Mobility

August 2018

vmware®

©2018 VMware, Inc.

Disclosure Statement

I'm a non-attorney spokesperson …….

The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

vmware®

©2018 VMware, Inc.

Who am I?

Introduction

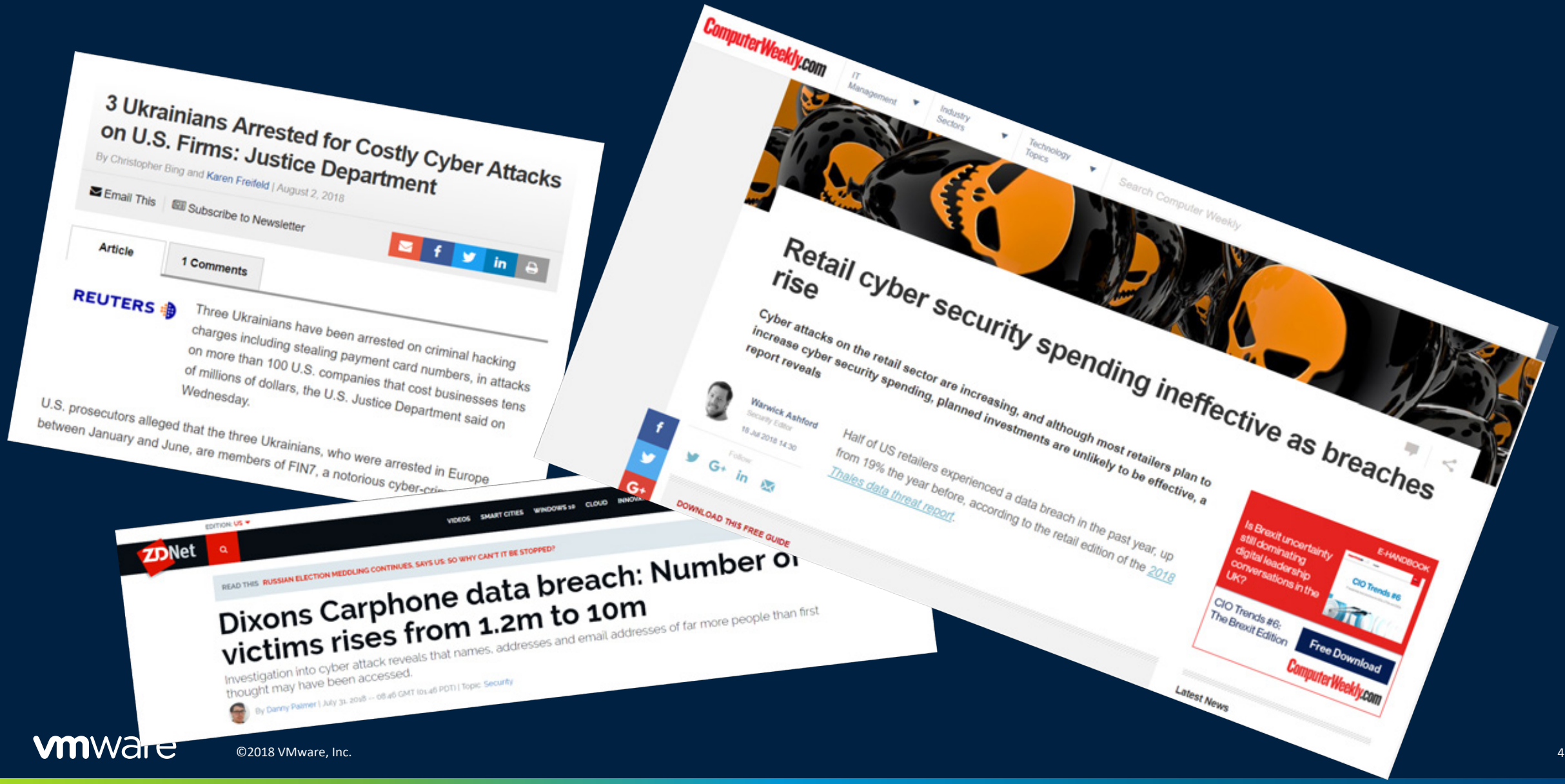
- Don Bailey: VMWare Solutions Architect – National Security

- Prior to joining VMware:

©2018 VMware, Inc.

Despite Significant Increases in Cybersecurity Spending Incidents of Breaches Rise

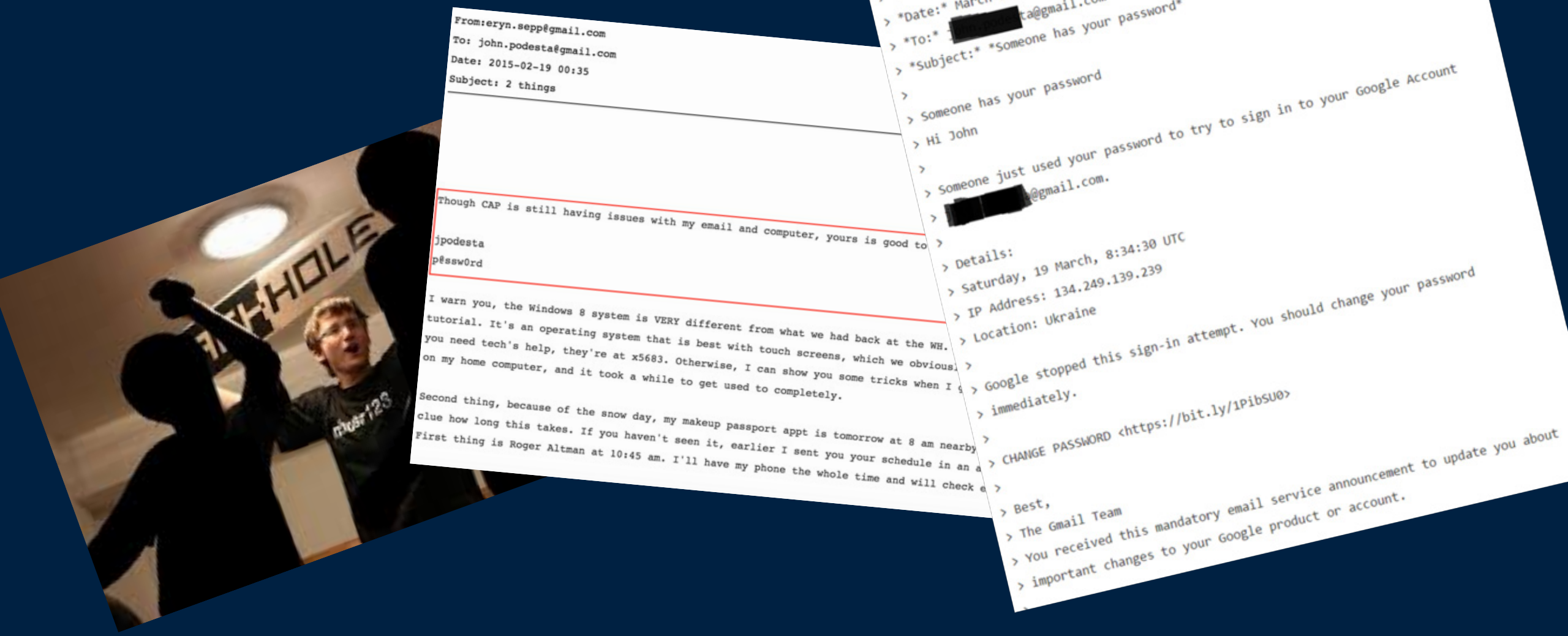
Clearly What We, Collectively, are Doing in Cybersecurity is Not Working



©2018 VMware, Inc.

Sometimes We Meet the Problem …

And the Problem is Us ….



©2018 VMware, Inc.

The Cybersecurity Conundrum

- The estimated compound annual growth rate (CAGR) in Cybersecurity spending is 8.7% through 2020
- The annual number of data breaches in the U.S. last year hit an all-time record high
  - 1,093 breaches – a 40% increase over the previous year
  - Corporations and Governments worldwide are losing ~$500B per year due to data breaches
- No shortage of guidance
- Complexity is overwhelming
- Change is constant
- Automation is out-of-reach
- Responding to alerts is onerous

vmware®
©2018 VMware, Inc.

Anatomy of an Attack

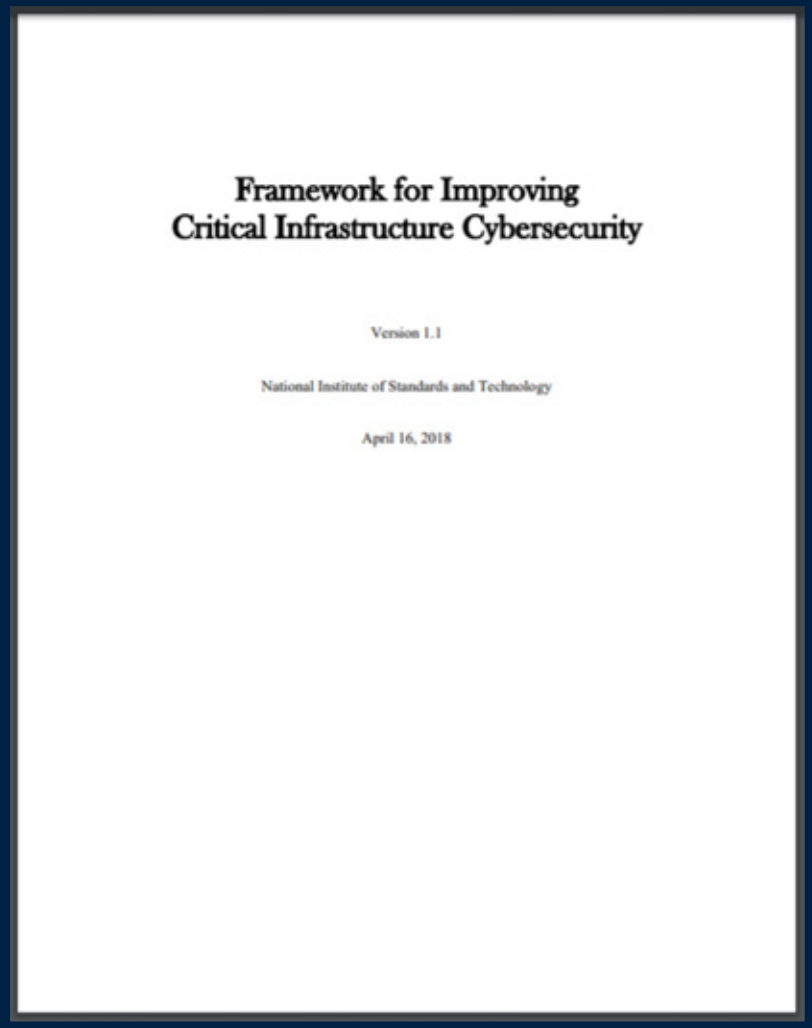
OPM – Target – Sony – etc.

- Reconnaissance
  - Passive Reconnaissance
  - Active Reconnaissance
    - In the OPM attack this phase lasted 5 months
- Exploitation
  - Leverage Information Gathered During Reconnaissance to Gain Access to Target
    - In some cases systems are exploited for an extended period of time
- Exfiltration
  - Establishment and Use of Drop-point Repositories
- Clean-up Tracks
  - Scrub, Alter, or Delete Specific Log Files

vmware®
©2018 VMware, Inc.

NIST Cyber Security Framework

They Clearly Need to Tone Down Their Graphics Art Dept.



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

©2018 VMware, Inc.

NIST CSF Core

©2018 VMware, Inc.

Two Steps to More Effective Security

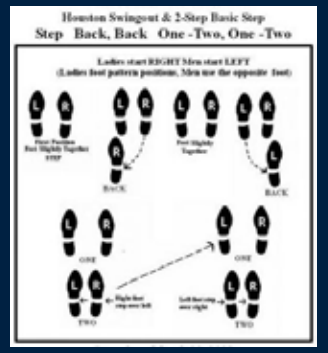
Implement Core Principals & Focus on Protecting Critical Apps

- Implement Core Principals of Cybersecurity Hygiene
  - Least Privilege
  - Micro-segmentation
  - Encryption
  - Multi-Factor Authentication
  - Patching
- Focus on Protecting *Individual* Critical Applications
  - Take a Risk-based Approach
  - Get More Specific
  - Control Access to Each Individual Application
  - Monitor with Specific Knowledge of the Application

©2018 VMware, Inc.

Step One – Implement Core Principals

Least Privilege



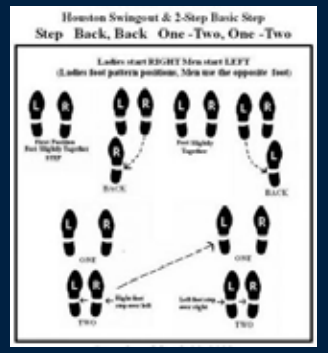
- Least Privilege

Users should be allowed only the minimum necessary access needed to perform their job and nothing more. And system components should be allowed only the minimum necessary function needed to perform their purpose and nothing more.

©2018 VMware, Inc.

Step One – Implement Core Principals

Least Privilege



- Least Privilege

Users should be allowed only the minimum necessary access needed to perform their job and nothing more. And system components should be allowed only the minimum necessary function needed to perform their purpose and nothing more.

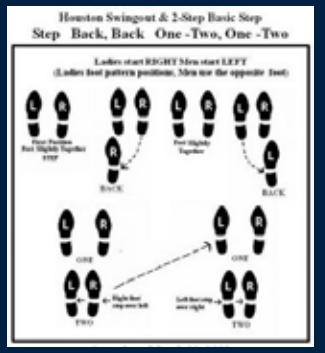
- Major Breach Where Core Principal Not Properly Implemented

If a least privilege environment has not been effectively implemented and users are provided with higher levels of access then they need, attackers can steal these credentials (user name and password) and gain broad access to systems.
For example, in the Target and Sony breaches, attackers were able to gain administrative-level privileges.

©2018 VMware, Inc.

Step One – Implement Core Principals

Micro-segmentation



- Micro-segmentation

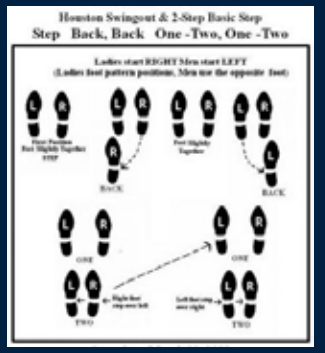
The whole IT environment should be divided into small parts to make it more manageable to protect and to contain the damage if one part gets compromised.

Protecting the IT environment by breaking it up into smaller parts is similar to the use of compartments on a ship. It makes the ship easier to protect. If the ship is damaged in one area, the damage is contained to that area.

©2018 VMware, Inc.

Step One – Implement Core Principals

Micro-segmentation



- Micro-segmentation

The whole IT environment should be divided into small parts to make it more manageable to protect and to contain the damage if one part gets compromised.
Protecting the IT environment by breaking it up into smaller parts is similar to the use of compartments on a ship. It makes the ship easier to protect. If the ship is damaged in one area, the damage is contained to that area.

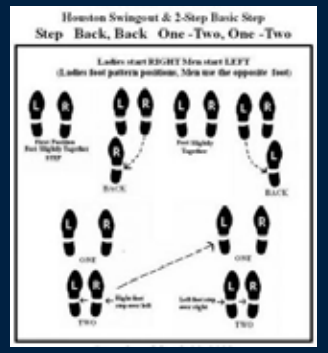
- Major Breach Where Core Principal Not Properly Implemented

If micro-segmentation has not been effectively implemented, attackers can break into one part of the network and then easily move around to other parts.
For example, in the Target breach, after an initial intrusion into the HVAC system, the attackers were able to move around to the payment network system. In the Sony breach, the attackers were also able to move around from one part of the network to another. In the case of the OPM breach, the attackers obtained access to OPM's local area network and then pivoted to the Interior Department's data center.

©2018 VMware, Inc.

Step One – Implement Core Principals

Encryption



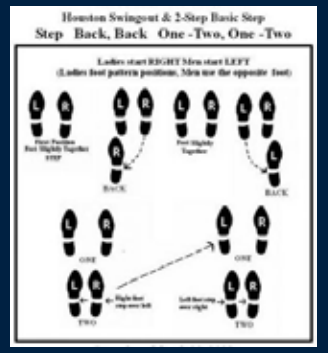
- Encryption

For critical business processes, all data should be encrypted, while stored or transmitted. In the event of a data breach, stealing critical files should only result in obtaining unreadable data.

©2018 VMware, Inc.

Step One – Implement Core Principals

Encryption



- Encryption

For critical business processes, all data should be encrypted, while stored or transmitted. In the event of a data breach, stealing critical files should only result in obtaining unreadable data.

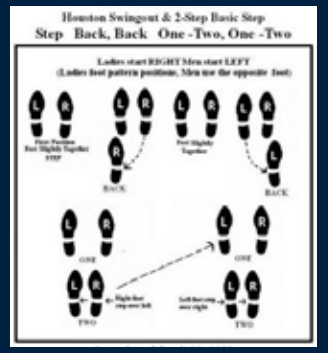
- Major Breach Where Core Principal Not Properly Implemented

If encryption has not been effectively implemented, attackers can exfiltrate data in readable form.
For example, after a data breach at Royal & Sun Alliance Insurance PLC, government investigators determined that the company had not adequately encrypted the data. Shockingly, the data exposed in the OMB breach was not encrypted.

©2018 VMware, Inc.

Step One – Implement Core Principals

Multi-Factor Authentication



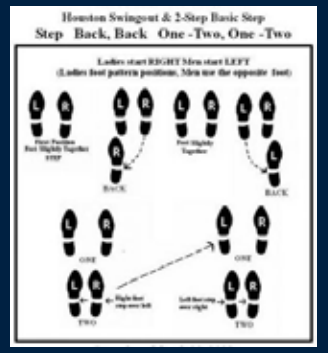
- Multi-Factor Authentication

The identity of users and system components should be verified using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function

©2018 VMware, Inc.

Step One – Implement Core Principals

Multi-Factor Authentication



- Multi-Factor Authentication

The identity of users and system components should be verified using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function

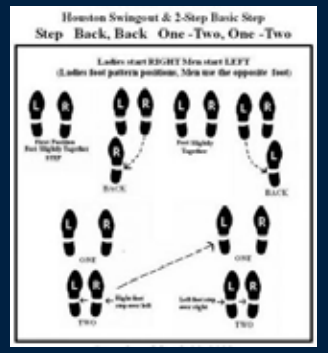
- Major Breach Where Core Principal Not Properly Implemented

If multi-factor authentication (MFA) is not effectively implemented, attackers can obtain passwords and use them to access systems.
For example, in the OPM breach, if the contractor logons had been enforced with a risk appropriate level of MFA it would have limited the ability of the attackers to use the stolen credentials of the government contractor. In the case of the breach at LinkedIn, the hack exposed inadequately protected passwords of 100 million users. Since consumers often use passwords on multiple sites, MFA would have reduced the risk.

©2018 VMware, Inc.

Step One – Implement Core Principals

Patching



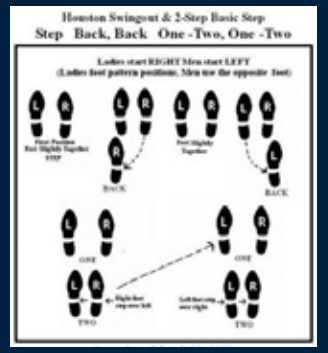
- Patching

Systems should be kept up to date and consistently maintained. Any critical system that is out of date is a meaningful security risk.

©2018 VMware, Inc.

Step One – Implement Core Principals

Patching



- Patching

Systems should be kept up to date and consistently maintained. Any critical system that is out of date is a meaningful security risk.

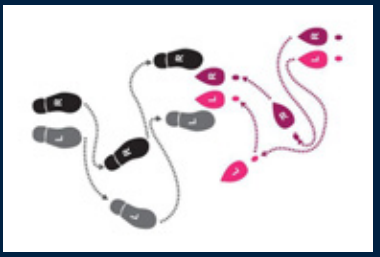
- Major Breach Where Core Principal Not Properly Implemented

If patching is not effectively implemented, attackers can exploit open holes in systems.
For example, the WannaCry ransomware exploited a known software vulnerability for which a patch was available. Organizations that fell victim had failed to effectively patch.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Step Two Will Make It Easier to Effectively Implement the Core Principals

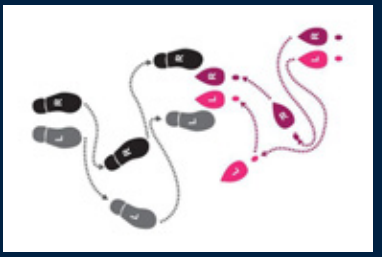


The next step is to focus on protecting *individual* critical applications. This will make it easier to effectively implement the core principles of cyber hygiene.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Step Two Will Make It Easier to Effectively Implement the Core Principals



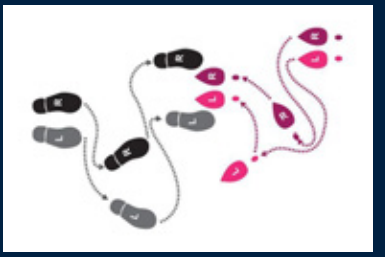
The next step is to focus on protecting *individual* critical applications. This will make it easier to effectively implement the core principles of cyber hygiene.

Focusing on critical applications puts the focus where it should be: on the crown jewels. Ultimately, an organization's crown jewels are its mission-critical business applications and the data within them. Examples include: an enterprise financial application that processes sensitive data in creating the company's financial statements; an ordering application that fulfills customer orders, including storing personal information and credit card data; an HR application that contains confidential employee data; and an R&D application that contains trade secrets. The application is the mechanism for accessing and interacting with the data.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Step Two Will Make It Easier to Effectively Implement the Core Principals



The next step is to focus on protecting *individual* critical applications. This will make it easier to effectively implement the core principles of cyber hygiene.

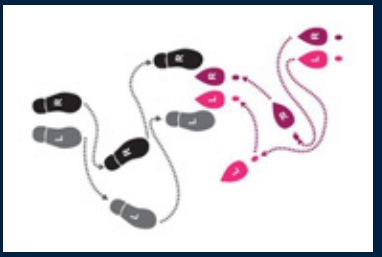
Focusing on critical applications puts the focus where it should be: on the crown jewels. Ultimately, an organization's crown jewels are its mission-critical business applications and the data within them. Examples include: an enterprise financial application that processes sensitive data in creating the company's financial statements; an ordering application that fulfills customer orders, including storing personal information and credit card data; an HR application that contains confidential employee data; and an R&D application that contains trade secrets. The application is the mechanism for accessing and interacting with the data.

Even though the goal of information security is to protect these crown jewels, current approaches are focused on protecting the IT infrastructure, like routers (hardware that routes traffic on a network) or servers (computers that provide processing power). Protecting the IT infrastructure is necessary but not sufficient.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Take a Risk-based Approach

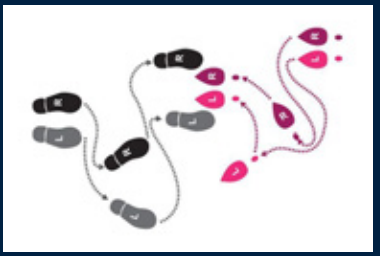


It is the critical applications and data that are of the value to the business. The compromise of these assets represents significant risk for the organization. The infrastructure provides the things an application needs to operate but is not itself the critical asset.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Get More Specific

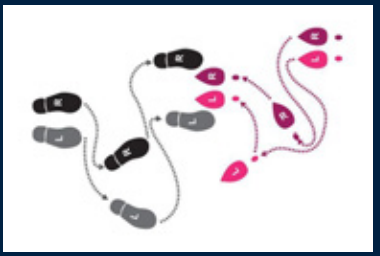


Focusing security on the infrastructure isn't specific enough. It's like trying to protect all the houses in a community by putting a fence around them with a locked gate. It would be more effective if you focused on protecting each individual house.
asset.

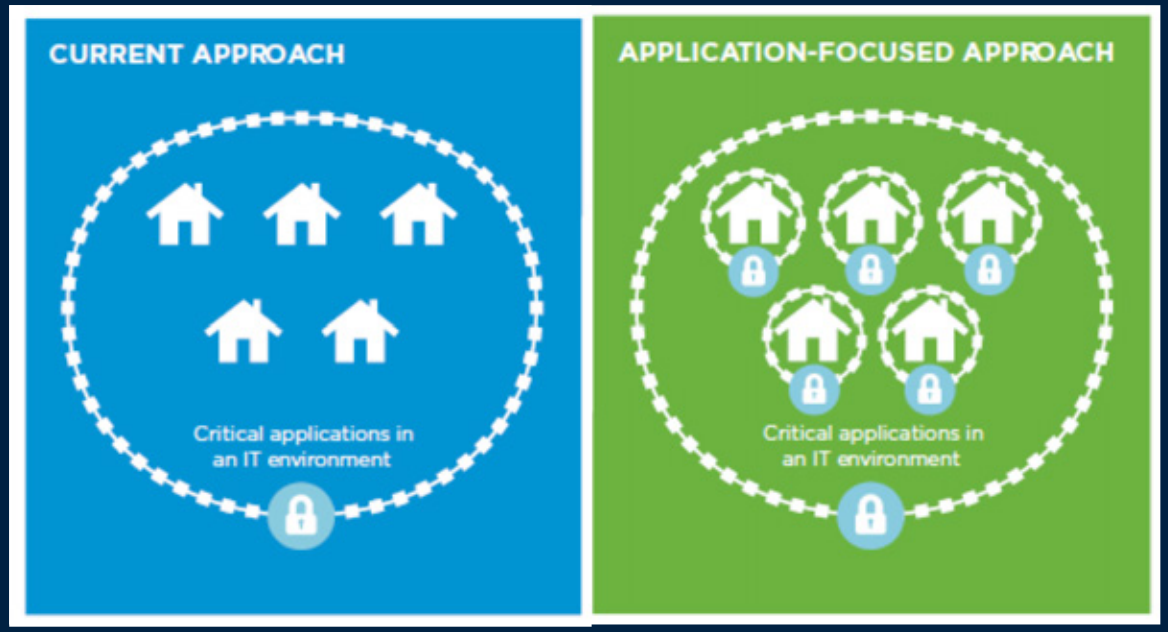
©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Get More Specific



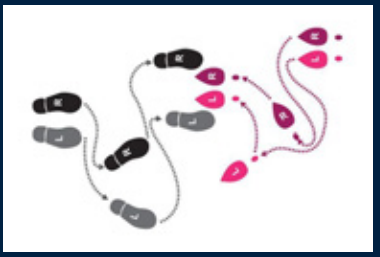
Focusing security on the infrastructure isn't specific enough. It's like trying to protect all the houses in a community by putting a fence around them with a locked gate. It would be more effective if you focused on protecting each individual house.
asset.



©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Control Access to Each Critical Application

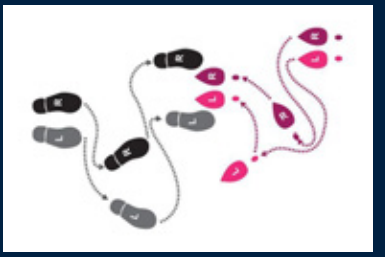


With current approaches, it's hard to effectively achieve security goals, such as ensuring only minimum necessary access. For example, a firewall is often set up at the perimeter of the whole enterprise (like the fence around our whole community) to control access to a group of applications, which can often be thousands of applications. Instead, there should be a firewall set up to control access to each individual critical application (like each individual house), allowing only access by the users and system components that absolutely need access to that one application (house).

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Control Access to Each Critical Application



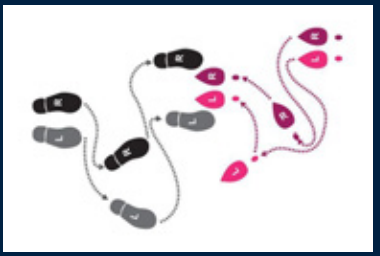
With current approaches, it's hard to effectively achieve security goals, such as ensuring only minimum necessary access. For example, a firewall is often set up at the perimeter of the whole enterprise (like the fence around our whole community) to control access to a group of applications, which can often be thousands of applications. Instead, there should be a firewall set up to control access to each individual critical application (like each individual house), allowing only access by the users and system components that absolutely need access to that one application (house).

Security also needs to get more efficient. Imagine that the guards at the gate get a phone call alerting them to unusual activity somewhere in the community. The guards might spend all day looking around the community looking for the unusual activity. It would be more efficient if the guards knew exactly which house to go to, if the house was empty or filled with valuables, and if the activity was normal for that house.

©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Monitor with Specific Knowledge of the Application

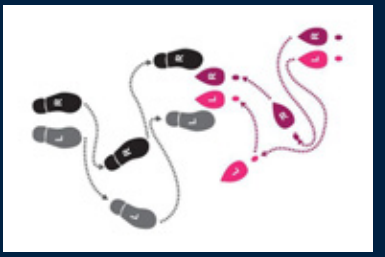


This is similar to information security monitoring systems. They typically send out an alert indicating an intrusion into the network or part of the network with no specifics on the application. The cybersecurity team has to spend a lot of time investigating. It would be better if the alert would indicate which application was affected, how critical it was, and if the activity detected was legitimate for that application.

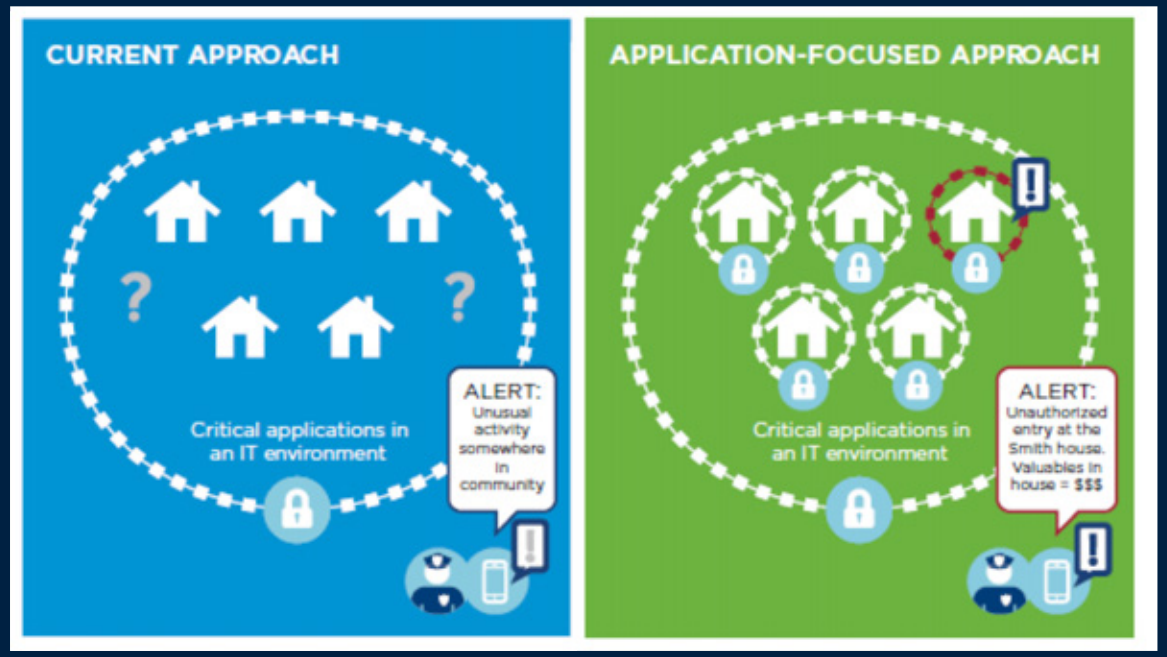
©2018 VMware, Inc.

Step Two – Focus on Protecting *Individual* Critical Applications

Monitor with Specific Knowledge of the Application



This is similar to information security monitoring systems. They typically send out an alert indicating an intrusion into the network or part of the network with no specifics on the application. The cybersecurity team has to spend a lot of time investigating. It would be better if the alert would indicate which application was affected, how critical it was, and if the activity detected was legitimate for that application.



©2018 VMware, Inc.

Thank You

vmware®

©2018 VMware, Inc.