

Cyber Risk = Disruptive Business Risk

Feb 2, 2021

 **HCCA™**
Health Care Compliance Association

Cyber Risk = Disruptive Business Risk







  **Ali Pabrai**
Global Cybersecurity & Compliance Expert



1

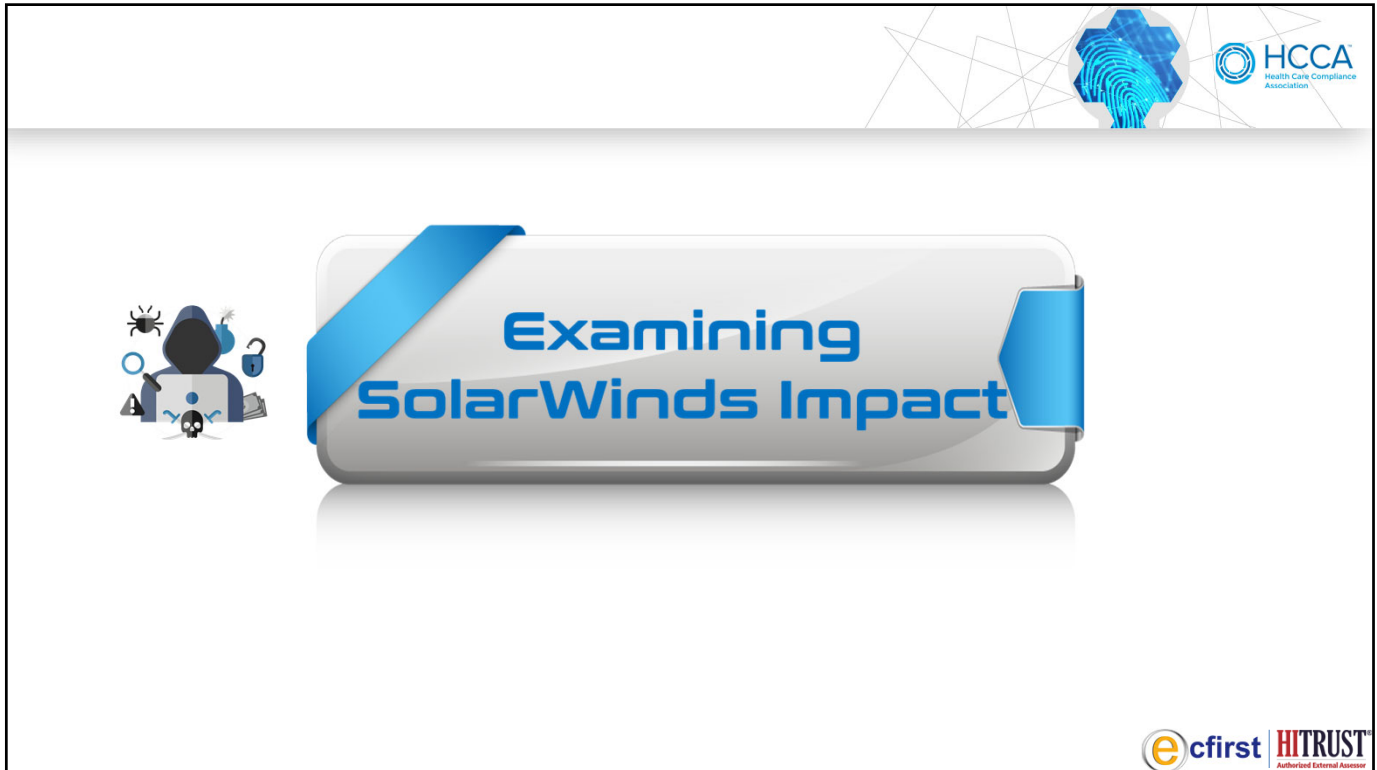
Agenda



Learning Objectives

- 1. Examine disruptive cyber threats including ransomware, phishing, DoS, DDoS.
- 2. Step thru how to establish an audit-ready compliance program.
- 3. Analyze critical areas to address in an enterprise security plan.

2



The graphic features a central white banner with a blue ribbon effect, containing the text "Examining SolarWinds Impact" in blue. To the left of the banner is an icon of a hacker with a laptop, a spider, and a padlock. In the top right corner, there are logos for HCCA (Health Care Compliance Association), ecfirst, and HITRUST (Authorized External Assessor). The background includes a network diagram and a fingerprint icon.

3

Cyber Threat Is Real and Growing

Hackers used a *supply chain attack*, exploiting SolarWinds management software updates to insert malicious code on the targets' servers

- ☒ SolarWinds breach could be the most significant cyber incident in American history.
- ☒ A sophisticated, smart and savvy attack.
- ☒ SolarWinds has more than **300,000 customers, including 400 companies in the Fortune 500.**
- ☒ It appears that this was purely an intelligence-gathering effort.
- ☒ What is truly scary is that the **Russians** are inside the house now. Turning off the system and uninstalling SolarWinds software isn't enough.
- ☒ It may take years and thousands of hours to unpack fully where the Russians hid themselves and their code.
- ☒ The suspected Russian hack that compromised parts of the U.S. government was executed with a scope and sophistication that has surprised even veteran security experts and exposed a potentially critical vulnerability in America's technology infrastructure.

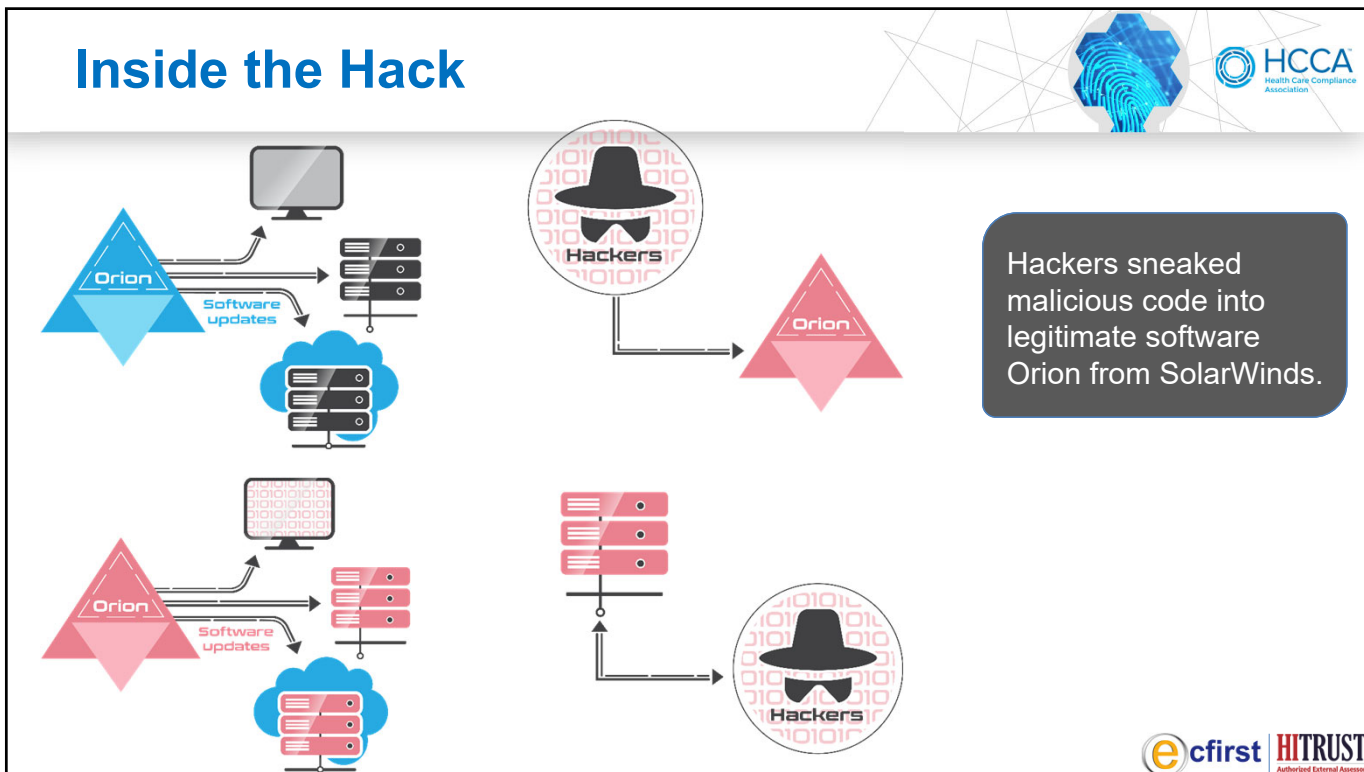


The graphic features a central white box with a blue border containing the text "Hackers used a supply chain attack, exploiting SolarWinds management software updates to insert malicious code on the targets' servers". Below this is a list of seven bullet points, each starting with a blue square icon containing a white 'r'. In the top right corner, there are logos for HCCA (Health Care Compliance Association), ecfirst, and HITRUST (Authorized External Assessor). The background includes a network diagram and a fingerprint icon.

4

Cyber Risk = Disruptive Business Risk

Inside the Hack



5

Global State of Cybersecurity

Sun Tzu

“Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win”

The Art of War

6

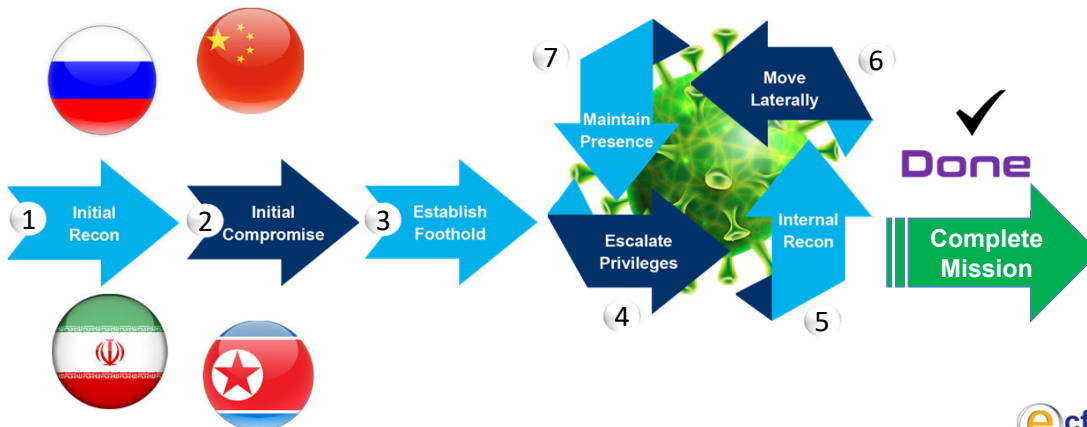
Cyber Risk = Disruptive Business Risk

Cyber-attacks: Global & Sophisticated



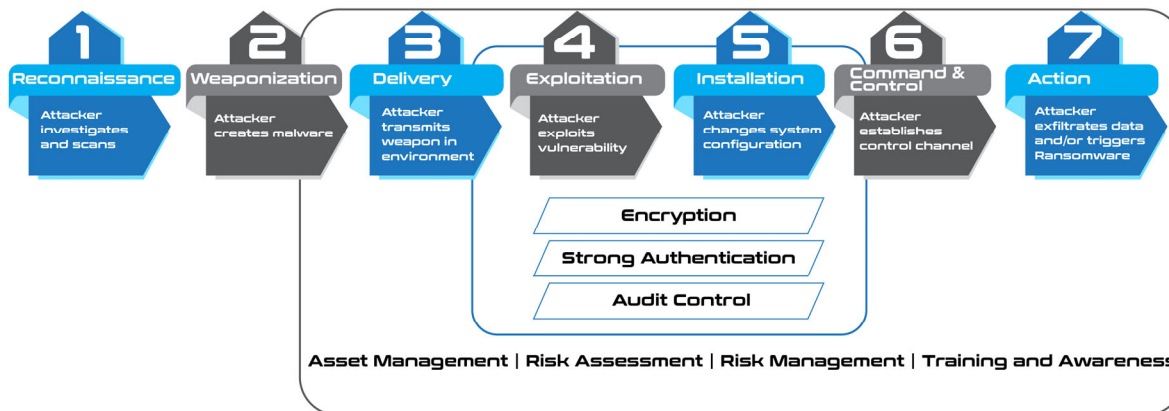
COVID-19 Disrupts Business

The world has emerged flatter, as we witness COVID-19 disrupt business. Cyber strategy now defined in two words, *cyber resilience*.



7

Cyber-attacks: Global & Sophisticated



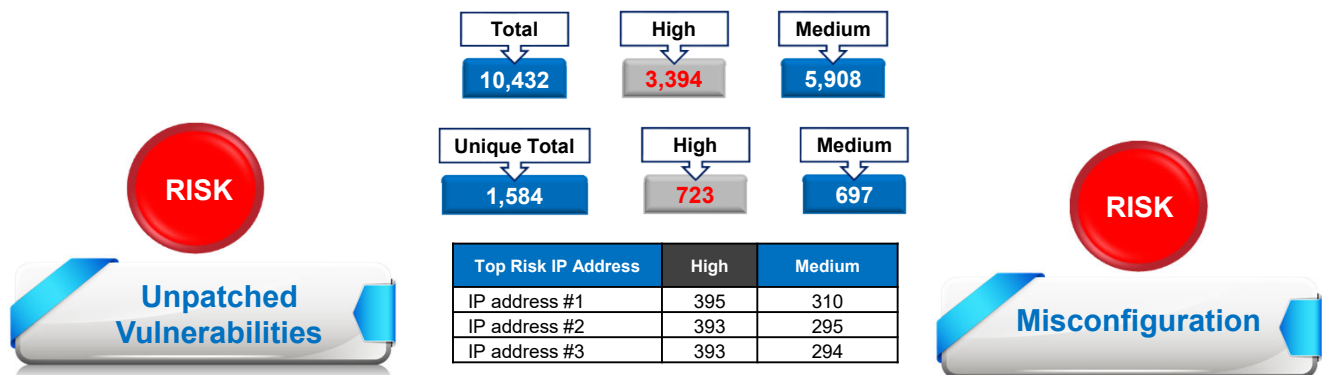
8

Asymmetric Attacks



9

2020 Client Cyber Assessment



10

2020 Client Cyber Assessment



Allow an attacker to gain unauthorized access to sensitive data



Allow an attacker to perform a Denial of Service attack



Allow an attacker to take control of the system



Provide an attacker with valuable information



Allow an attacker to gain elevated privileges



Allow an attacker to gain access to sensitive data



Allow an attacker to bypass security restrictions



1,440

Unique vulnerabilities, per organization



140,000

Vulnerabilities recorded.



11

Ransomware and Cryptojacking



A new organization fell victim to ransomware every 14 seconds in past years, and every 11 seconds by 2021.

In recent years, ransomware from phishing emails increased 109%.



Malicious coin mining or "cryptojacking" is the act of installing a cryptocurrency thus enslaving their device to slowly gather coins for the attacker



12

IoT + DDoS = High Business RISK



- The global IoT market is forecast to be worth **\$1.7T** in recent years.
- More than **80%** of **senior executives** across industries, on average, say IoT is critical to some or all lines of their business in recent years.



DDoS attack speeds exceed 1.5 Tbps!



127 new IoT devices connect to the internet every second.



Nearly **13 billion** IoT sensors and devices in use in the consumer segment.



Prepared for
SB 327


California



13

Phishing



77% of successful social engineering attacks start with a phishing email. 



More than **90%** of successful hacks and data breaches start with phishing scams.



Healthcare and pharmaceutical organizations had the highest percentage of phishing attacks at **44.7%**.



Cybercriminals ramped up COVID-19 related phishing attacks over **667%** March 2020.



14



Compliance Mandates

Sun Tzu

"In the midst of chaos, there is also opportunity"

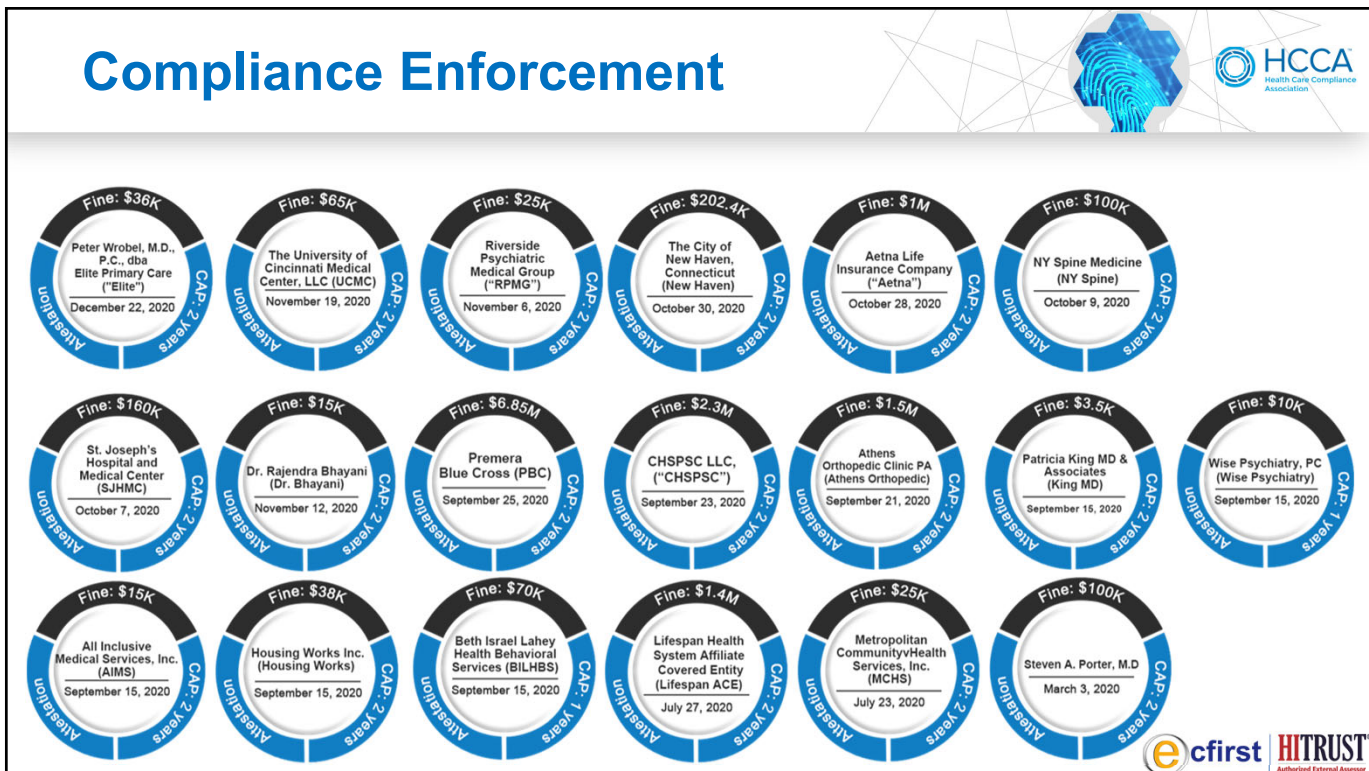
The Art of War

HCCA Health Care Compliance Association

ecfirst HITRUST Authorized External Assessor

15

Compliance Enforcement



EntityDate	Fine	Assessment	Cap
Peter Wrobel, M.D., P.C., dba Elite Primary Care ("Elite") December 22, 2020	\$36K	Attestation	2 years
The University of Cincinnati Medical Center, LLC (UCMC) November 19, 2020	\$65K	Attestation	2 years
Riverside Psychiatric Medical Group ("RPMG") November 6, 2020	\$25K	Attestation	2 years
The City of New Haven, Connecticut (New Haven) October 30, 2020	\$202.4K	Attestation	2 years
Aetna Life Insurance Company ("Aetna") October 28, 2020	\$1M	Attestation	2 years
NY Spine Medicine (NY Spine) October 9, 2020	\$100K	Attestation	2 years
St. Joseph's Hospital and Medical Center (SJHMC) October 7, 2020	\$160K	Attestation	2 years
Dr. Rajendra Bhayani (Dr. Bhayani) November 12, 2020	\$15K	Attestation	2 years
Premera Blue Cross (PBC) September 25, 2020	\$6.85M	Attestation	2 years
CHSPSC LLC, ("CHSPSC") September 23, 2020	\$2.3M	Attestation	2 years
Athens Orthopedic Clinic PA (Athens Orthopedic) September 21, 2020	\$1.5M	Attestation	2 years
Patricia King MD & Associates (King MD) September 15, 2020	\$3.5K	Attestation	2 years
Wise Psychiatry, PC (Wise Psychiatry) September 15, 2020	\$10K	Attestation	1 year
All Inclusive Medical Services, Inc. (AIMS) September 15, 2020	\$15K	Attestation	2 years
Housing Works Inc. (Housing Works) September 15, 2020	\$38K	Attestation	2 years
Beth Israel Lahey Health Behavioral Services (BILHBS) September 15, 2020	\$70K	Attestation	1 year
Lifespan Health System Affiliate Covered Entity (Lifespan ACE) July 27, 2020	\$1.4M	Attestation	2 years
Metropolitan Community Health Services, Inc. (MCHS) July 23, 2020	\$25K	Attestation	2 years
Steven A. Porter, M.D. March 3, 2020	\$100K	Attestation	2 years

HCCA Health Care Compliance Association

ecfirst HITRUST Authorized External Assessor

16

Active Cyber Database

California's SB 327: An IoT Cybersecurity Mandate

Key Facts

- Is effective January 1, 2020.
- Focused on security features of IoT devices to protect personal information.
- The California attorney general, county counsel and district attorneys will enforce the bill.
- Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.
- Allows law enforcement agencies to obtain connected device information from a manufacturer as authorized by law or court order.
- Manufacturers need to consider how to deal with post-market security issues, such as patching vulnerabilities with software updates.

SB 327 - Information Privacy: Connected Devices

A manufacturer of a connected device shall equip the device with a reasonable security feature:

- Appropriate to the nature and function of the device.
- Appropriate to the information it may collect, contain, or transmit.
- "Connected device" is defined as devices or any other physical objects that can directly or indirectly connect to the internet and are assigned an IP or Bluetooth address.
- It does not apply to connected devices subject to security requirements under federal law, regulations or guidance promulgated by a federal agency.
- If a connected device is equipped with a means for authentication outside a network, it will be deemed a reasonable security feature, if either of the following requirements are met:
 - Preprogrammed password is unique to each device manufactured.
 - Device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.
- The Attorney General, a city attorney, a county counsel, or a district attorney have the exclusive authority to enforce this title.

Title 1.81.26: Security of Connected Devices

1798.91.04
Protect the device and any information from unauthorized access, destruction, use, modification, or disclosure.

1798.91.05
Verifying the authority of a user, process, or device to access resources in an information system.

1798.91.06
Not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications.

Key Actions Required

- Businesses should familiarize themselves with industry standards and applicable guidance relating to IoT device security.
- Businesses subject to compliance should now to build "security by design" into the manufacturing processes.

Cyber Resilience in the 2020s

Global Cybersecurity & Compliance Expert

17

NIST IR 8228

IoT Cybersecurity and Privacy Risks

IoT Device Capabilities

Transducer Capabilities	Interface Capabilities	Supporting Capabilities Examples
Sensing	API Application Interface	Device Management
Actuating	Human User Interface	Cybersecurity Capabilities
	Network Interface	Privacy Capabilities

Recommendations for Addressing Cybersecurity and Privacy Risk

Risk Considerations


- Device Interactions with the Physical World.
- Device Access, Management, and Monitoring Features.
- Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness.

18

Cyber Risk = Disruptive Business Risk

Active Cyber Defense


CCPA: America's GDPR



Key Facts

- Effective January 1, 2020.
- Enforced July 1, 2020.
- Privacy right of action for California residents.
- Grants new enforcement power to the Attorney General with high damages recoverable.

CCPA Best Practice



Who Needs to Comply?

If you are a for-profit business that collects personal information from CA residents and:



- Have annual gross revenue is above **\$25 million**.
- Alone or in combination annually buy, receive, sell or share the personal information of **50,000+** consumers.
- Derive **50%** or more of its annual revenue from selling consumers' personal information.

Consumer Rights

1. Abbreviated Disclosure Right Applicable to Businesses that Collect Personal Information.
2. Expanded Disclosure Right Applicable to Businesses that Collect Personal Information.
3. Right to Request Information from Businesses that Sell or Disclose Personal Information for a Business Purpose.
4. Right to Opt-Out of the Sale of Data.
5. Right to Opt-in for Children: Business Obligation Not to Sell Children's Personal Information Without Affirmative Authorization.
6. Deletion Rights.
7. Rights to Access and Portability.
8. Not to be Discriminated Against for Exercising Any of the Consumer's Rights under the Title.

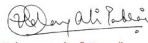
CCPA: California Consumer is the Focus

How Does CCPA Impact Consumers?		
Right to Knowledge	Right to be Forgotten	Right to Control Who has Access to their Information
<p>Consumers have the right to request information about:</p> <ul style="list-style-type: none"> What information a company is collecting about them. How that information will be used. If and with whom that information will be shared. 	<ul style="list-style-type: none"> Companies must delete all information they have about a consumer at the consumer's request. Exceptions include: <ul style="list-style-type: none"> Data being processed and retained to complete a consumer-requested transaction. Specific research purposes. Limited analytical used other regulatory and contractual exceptions. 	<p>Consumers must be able to opt out of the sale of their information to third parties.</p>





Code: CCPANH0002

Cyber Resilience
in the 2020s



Global Cybersecurity & Compliance Expert



19

Active Cyber Defense

ISO 27001: A Global Standard





ISO 27002
Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Access Control
Cryptography
Physical & Environmental Security
Operations Security
Communications Security
System Acquisition, Development & Maintenance
Supplier Relationships
Information Security Incident Management
Information Security Aspects of Business Continuity Management
Compliance





20





Cybersecurity Framework


Sun Tzu

"What the ancients called a clever fighter is one who not only wins, but excels in winning with ease"

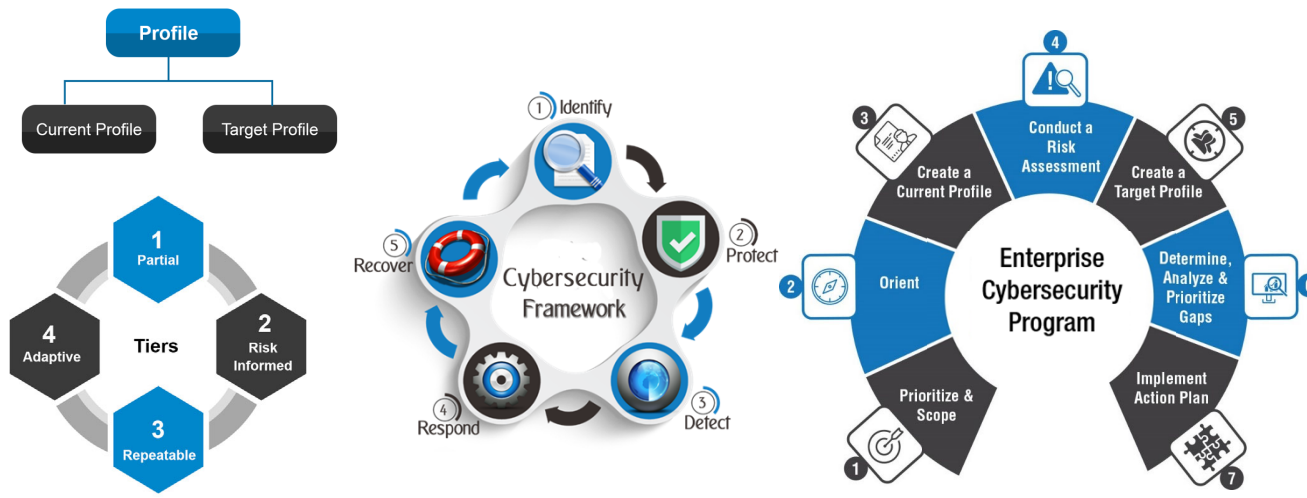
The Art of War



21




NIST Cybersecurity Framework



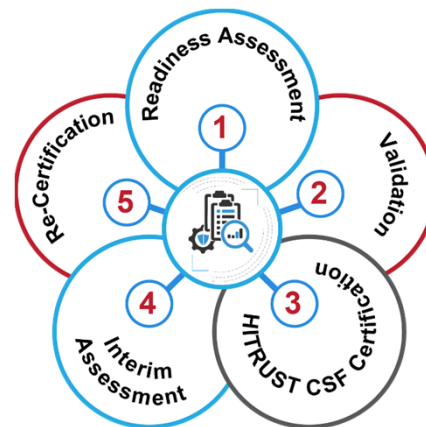
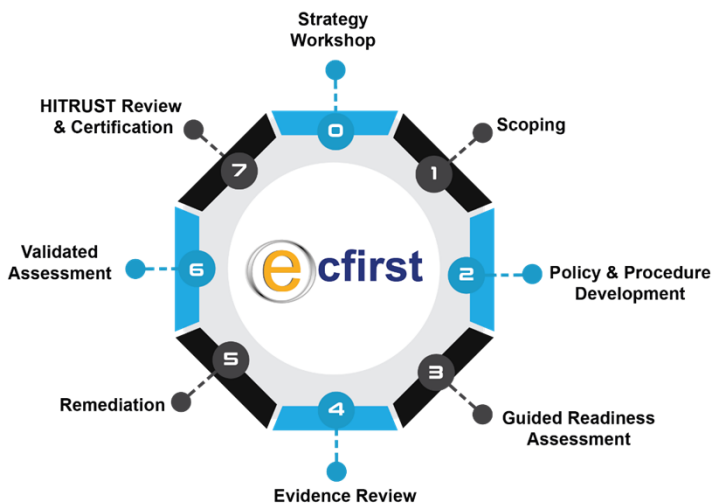
The diagram illustrates the NIST Cybersecurity Framework components:

- Profile:**
 - Current Profile
 - Target Profile
- Tiers:**
 - 1 Partial
 - 2 Risk Informed
 - 3 Repeatable
 - 4 Adaptive
- Cybersecurity Framework Core Functions:**
 - 1 Identify
 - 2 Protect
 - 3 Detect
 - 4 Respond
 - 5 Recover
- Enterprise Cybersecurity Program Process:**
 - 1 Prioritize & Scope
 - 2 Orient
 - 3 Create a Current Profile
 - 4 Conduct a Risk Assessment
 - 5 Create a Target Profile
 - 6 Determine, Analyze & Prioritize Gaps
 - 7 Implement Action Plan



22

HITRUST CSF Certification



23

CMMC: A New DoD Cyber Standard!



CMMC is a global cybersecurity standard that cybersecurity professionals must learn and keep up with.

- 17** Capability Domains
- 5** Maturity Levels
- 43** Capabilities
- 5** Processes
- 171** Practices

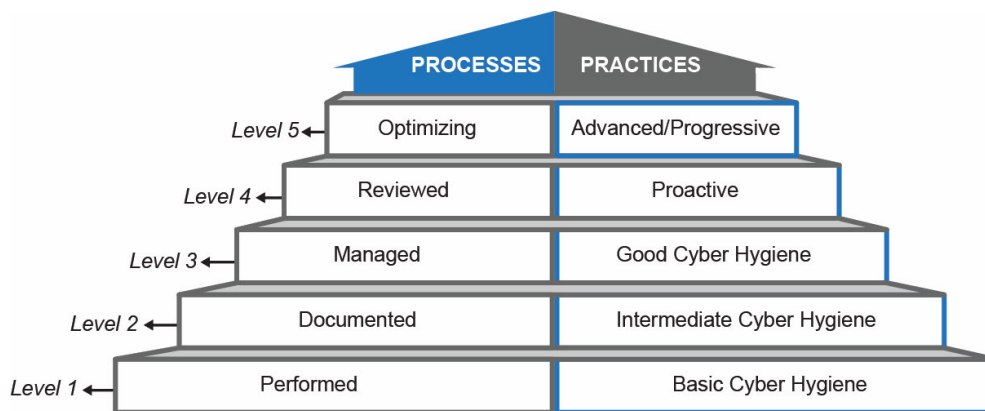
CMMC Level	# of Practices	Processes
L1	17	0 Process <ul style="list-style-type: none"> There are no maturity processes assessed at L1. An organization performs L1 practices but does not exhibit Institutionalization requirements.
L2	55	2 Processes <ul style="list-style-type: none"> Establish a policy that includes Domain requirements process institutionalization. Document the CMMC practices to implement the Domain requirement policy.
L3	58	1 Process <ul style="list-style-type: none"> Establish, maintain, and resource a plan that includes Domain requirement.
L4	26	1 Process <ul style="list-style-type: none"> Review and measure Domain requirements activities for effectiveness.
L5	15	1 Process <ul style="list-style-type: none"> Standardize a documented approach for Domain requirements across all applicable organizational units.
Total	171	5



24

CMMC Levels

- ❏ CMMC has five defined levels, each with a set of supporting practices and processes.
- ❏ To meet a specific CMMC level, an organization must meet the practices and processes within that level and below.



25

Getting Started: Key Steps



Sun Tzu

“The wise warrior avoids
the battle”

The Art of War



26

“If you define the problem correctly, you almost have the solution.”

STEVE JOBS

27

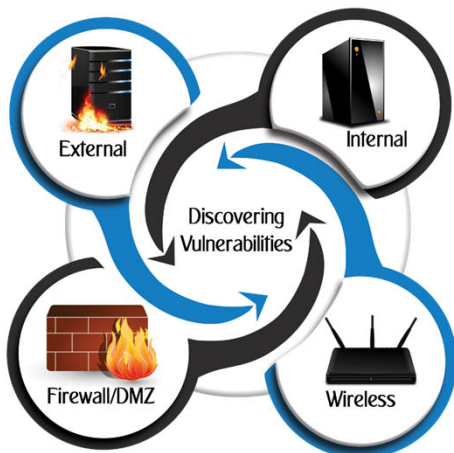
Risk Assessment



efirst HITRUST
Authorized External Assessor

28

Cyber Assessment



Conduct a Cybersecurity Assessment

1

Validate & Remediate Findings

2

Penetration Testing (Pen Test)

3

Pen Test



External Pen Test



Internal Pen Test



Web Application Pen Test



29

Cyber Incident Management Plan



Four Key Areas



Preparation



Detection & Analysis



Containment, Eradication, & Recovery



Post-Incident Activity

Sun Tzu

"Plan for what it is difficult while it is easy, do what is great while it is small!"

The Art of War



30

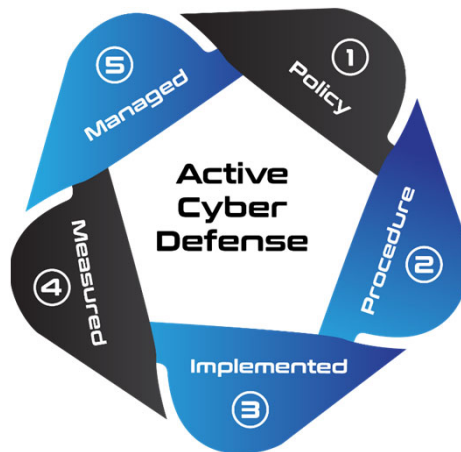
Cybersecurity Program



Cyber Immune Defense



Five Dimensions Aligned



31

Cyber Action Required Annually!



1. Implement a cybersecurity framework (e.g. NIST Cybersecurity Framework)
2. Conduct a comprehensive security risk assessment
3. Ensure a technical vulnerability assessment is performed quarterly & a pen test annually
4. Perform a Business Impact Analysis (BIA)
5. Develop a detailed Disaster Recovery Plan (DRP)
6. Create a cyber incident response plan
7. Active risk management program required



32

Cyber Risk = Disruptive Business Risk

About 



Consulting Practice



33

About 



Certification Training



34



Thank You!

@ Ali Pabrai | Ali.Pabrai@ecfirst.com

