Cybersecurity Resiliency for Defense Contractors Webinar Series:

Cyber Security: What Are Your Risks?

November 12, 2020
Jana White

ALPINE SECURITY IMEC

1

Today's Topics

- The NIST Cybersecurity Framework
  - *Identify – Protect – Detect – Respond – Recover*
- DoD-required Incident Response Plan

ALPINE SECURITY IMEC

2

ALPINE SECURITY

Service-Disabled Veteran Owned Small Business (SDVOSB)

Areas of Focus:

Cybersecurity Training

Penetration Testing

Vulnerability Assessments

CISO-as-a-Service

Cybersecurity Strategy

DFARS 252.204-7012 & CMMC

Based in Greater St. Louis Area

IMEC

3

Cybersecurity statistics

Quick Facts

- 73% of attacks by outsiders
- 50% by organized crime
- 58% victims are small businesses
- Time to compromise = minutes
- Time to detect = 100s of days
- Motivators: Money and Espionage
- Social attacks = nearly 50% of all breaches
  - Phishing and Pretexting = 98% of social attacks

Source: 2018 Verizon Data Breach Investigations Report

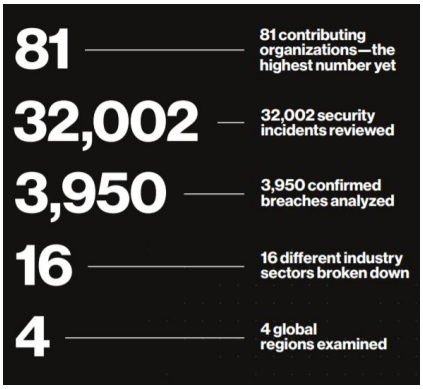
ALPINE SECURITY

IMEC

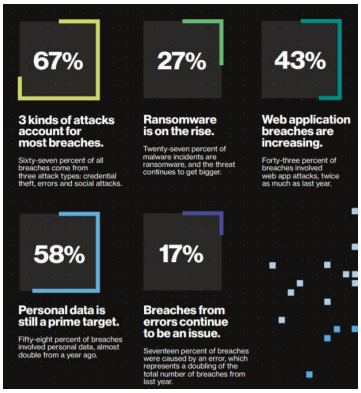
4

2020 Verizon DBIR

Most Comprehensive Report Ever



Top Insights of 2020



ALPINE SECURITY

IMEC

5

2020 Verizon DBIR -Manufacturing

- Frequency: 922 incidents, 381 with confirmed data disclosure
- Top Patterns: Crimeware, Web Applications and Privilege Misuse represent 64% of breaches
- Threat Actors: External (75%), Internal (25%), Partner (1%) (breaches)
- Actor Motives: Financial (73%), Espionage (27%) (breaches)
- Data Compromised: Credentials (55%), Personal (49%), Other (25%), Payment (20%) (breaches)
- Top Controls Needed: Boundary Defense, Implement a Security Awareness and Training Program, Data Protection

ALPINE SECURITY

IMEC

6

Crimeware – How it works

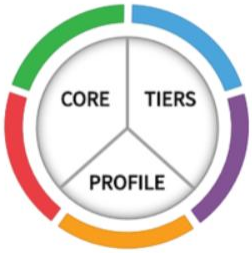
- Obtain password
- Infiltrate the network
- Download software
- Capture data

ALPINE SECURITY

IMEC

7

The NIST Cybersecurity Framework



The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

ALPINE SECURITY

IMEC

8

Framework Basics

The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities.

ALPINE SECURITY

IMEC

9

Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk.

The Framework Core consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

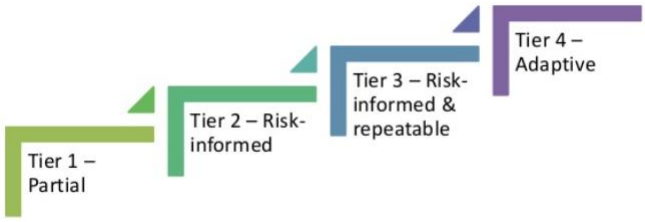
ALPINE SECURITY

IMEC

10

Framework Implementation Tiers

The Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.



Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.

ALPINE SECURITY

IMEC

11

Framework Profiles

A profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements, industry best practices, and reflects risk management priorities.

ALPINE SECURITY

IMEC

12

Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk (likelihood X impact)

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes

ALPINE SECURITY

IMEC

13

Framework Function - Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- *Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy*

ALPINE SECURITY

IMEC

14

Framework Function – Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

- *Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology*

ALPINE SECURITY

IMEC

15

Framework Function – Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- *Anomalies and Events; Security Continuous Monitoring; and Detection Processes*

ALPINE SECURITY

IMEC

16

Framework Function – Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

- *Response Planning; Communications; Analysis; Mitigation; and Improvements*

ALPINE SECURITY

IMEC

17

Framework Function – Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

- *Recovery Planning; Improvements; and Communications*

ALPINE SECURITY

IMEC

18

DoD-required Incident Response Plan

- You must rapidly report cyber incidents and cooperate with the DoD to respond to these security incidents, including providing access to affected media and submitting malicious software
- DFARS Clause 252.204-7012
  - *Safeguarding Covered Defense Information and Cyber Incident Reporting (highlights)*
  - ***Adequate security** (**The Contractor shall implement NIST SP 800-171**, as soon as practical, but not later than December 31, 2017)*
  - *If the Contractor intends to use an external cloud service provider …the **Contractor shall require and ensure that the cloud service provider meets security requirements** equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline*
  - ***Cyber incident reporting requirement (includes review for compromise, Rapidly report cyber incidents to DoD at https://dibnet.dod.mil., isolate malicious software in connection with a reported cyber incident***

ALPINE SECURITY

IMEC

19

What should be in my IRP? (A review)

- Organizations should document their guidelines for interactions with other organizations regarding incidents. (who, how, when)
- Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. (containment, training)
- Organizations should emphasize the importance of incident detection and analysis throughout the organization. (continuous monitoring)
- Organizations should create written guidelines for prioritizing incidents. (based on risk)

ALPINE SECURITY

IMEC

20

Incident response phases

The incident response phases are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

ALPINE SECURITY

IMEC

21

Incident Response Plan Dos and Don'ts

- Test incident response plan <u>at least</u> annually
- Properly and regularly train the staff with incident response responsibilities
- Set up alerts, follow up!
- Update and manage your incident response plan frequently
- Don't forget to include key stakeholders in the plan (executive management, service providers, business partners)
- Don't just put it on paper, ensure incident response becomes part of your business practice!

ALPINE SECURITY

IMEC

22

Have a ticketing/tracking system for cybersecurity incidents

- End users need to know how and when to report suspicious activity or incidents
- End users need to be trained on how to report cybersecurity incidents, and their response should be periodically tested (ex. phishing campaigns)
- A record of all reported suspicious activity or incidents should be maintained (and kept for historical record)
- All incidents should be assigned a criticality or priority score (based on risk), in case more than one incident needs to handled at a time
- All activities connected with a cybersecurity incident should be thoroughly documented, and a lessons learned report should be created after the incident has been resolved

ALPINE SECURITY

IMEC

23

Training your end users on your incident response plan

- Review your IRP with your team
- Create procedures for reporting suspicious activity or cybersecurity incidents (these should be accessible at all times)
- Have end users participate in incident response tabletop scenarios
- Tie your end user incident reporting training in with your other security awareness training (repetition of information and reinforcement of concepts)

IMEC

24

Creating a CIRT

To properly prepare for and address cybersecurity incidents your organization needs to have a centralized cybersecurity incident response team (CIRT). This team is responsible for analyzing security breaches and taking any necessary responsive measures to incidents.

- Your team should include an incident response manager, security analysts, IT and can include executive management, HR, legal, and public relations personnel
- Have a strong communication plan, designate the IR manager as the central point of communication

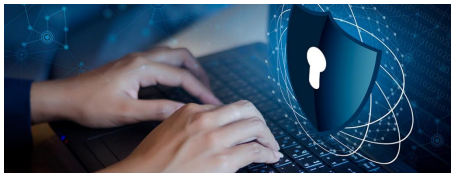
ALPINE SECURITY

IMEC

25

Key Responsibilities of your CIRT

- Creating and maintaining an incident response plan (IRP)
- Investigating and analyzing incidents
- Managing internal communications and updates during or immediately after incidents
- Communicating with employees, shareholders, customers, and the press about incidents as needed
- Remediating incidents
- Recommending technology, policy, governance, and training changes after security incidents



ALPINE SECURITY

IMEC

26

MSPs and your CIRT

- If you outsource your IT to an MSP (managed service provider), ensure that they are part of your CIRT
- Someone from your organization should head up your CIRT, provide support and enforce accountability
- Have MSP CIRT members participate in your incident response training and tabletop exercises
- **Ensure that your MSP is also DFARS compliant**, they handle your CUI Information System and your CUI

ALPINE SECURITY

IMEC

27

Developing Playbooks

Incident response playbooks are designed to provide a step-by-step walk-through for the most likely and impactful cybersecurity threats to your organization.

A playbook will ensure that the steps of the Incident Response Plan are followed appropriately and completely. Templates are recommended as a good starting point when developing your own playbooks.

ALPINE SECURITY

IMEC

28

Training your CIRT

- Review your IRP and your incident reporting procedures
- Train the team on the roles and responsibilities for entire CIRT
- Train the team communications plan
- Use your playbooks for training and tabletop scenarios
- Provide your CIRT with specialized cybersecurity training or certifications
- Provide CIRT training at least annually (update training each time!)

ALPINE SECURITY

IMEC

29

Run Tabletop Simulations

- Develop hypothetical scenarios
- Have a meeting with entire team (half or full day session is recommended. You can cover 2-3 scenarios in a full day session)
- Run the scenarios, make notes of what does and does not work as intended (have a dedicated person take notes throughout the day)
- **Update your IRP** to fix anything that did not work, or to include missing steps that were identified during the tabletop scenarios (including training needed!)

ALPINE SECURITY

IMEC

30

Update your IRP often!!!

ALPINE SECURITY

IMEC

31

Other Helpful Resources (Freebies!)

- NIST Cybersecurity Framework Online Learning - https://www.nist.gov/cyberframework/online-learning
- NIST Cybersecurity Framework v 1.1 - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST Cybersecurity Framework version 1.1 Manufacturing Profile (for manufacturers) - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf
- Incident Response Playbooks - https://www.incidentresponse.com/playbooks/

ALPINE SECURITY

IMEC

32

What We Covered Today…

- The NIST Cybersecurity Framework
  - *Identify – Protect – Detect – Respond – Recover*
- DoD-required Incident Response Plan

33

Jana White
jana.white@alpinesecurity.com
www.alpinesecurity.com
info@alpinesecurity.com
(844) 925-7463

34