SILICON PLAINS

IT - Cybersecurity - Compliance

Herb Miner
B.S. Computer Systems Engineering
MBA
Co-Founder and Chief Operations Officer
Silicon Plains, LLC

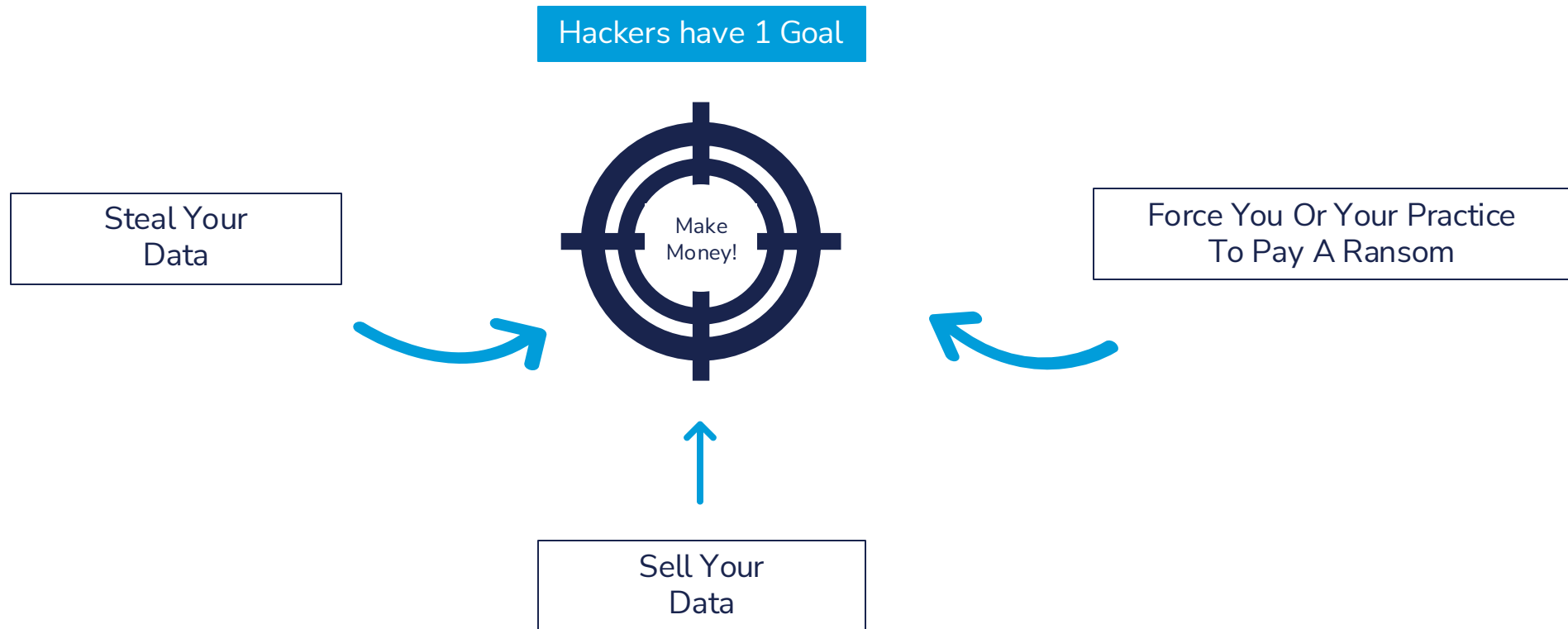**siliconplains.net - 877-287-7762 - herb@siliconplains.net**

About

- 35 Space Shuttle missions
- 16 satellite missions
- Instrument-rated with a private pilot's license
- Lockheed Martin
- NASA
- Department of Defense
- National Oceanic and Atmospheric Administration
- Silicon Plains, LLC - founded in 2009
  - Virtual Chief Information Officer services
  - Cyber Security and Compliance services
  - Consulting
- Prior Experience
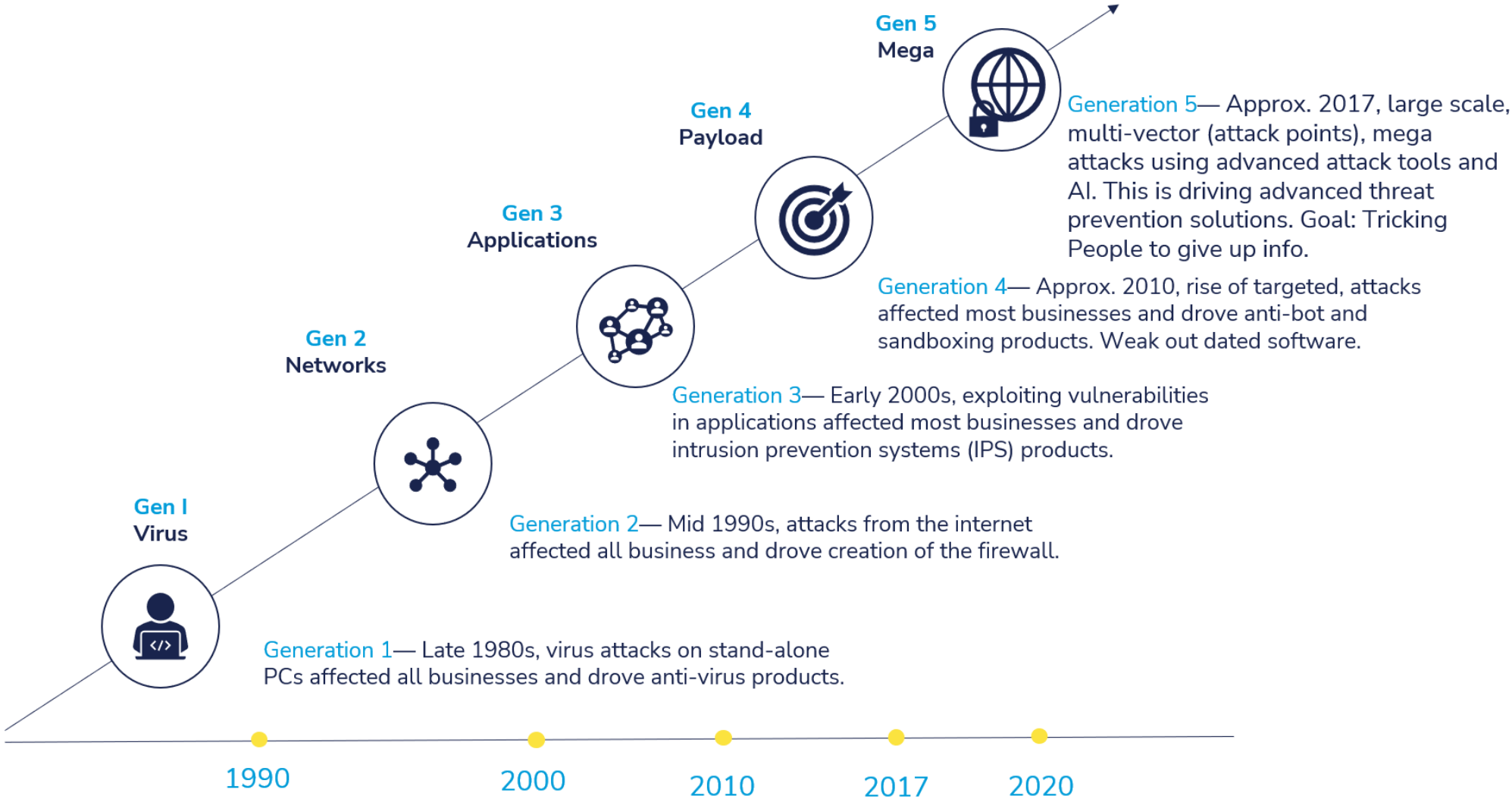 - Transportation and Logistics
  - Retail
  - Service industries

Cybersecurity and Compliance

## Why Should I Care?

Your Business is At Risk!

Hackers have 1 Goal

Make Money!

Steal Your Data

Force You Or Your Practice To Pay A Ransom

Sell Your Data

Current Cybersecurity Threats

Gen 5
Mega

Gen 4
Payload

Gen 3
Applications

Gen 2
Networks

Gen I
Virus

Generation 5— Approx. 2017, large scale, multi-vector (attack points), mega attacks using advanced attack tools and AI. This is driving advanced threat prevention solutions. Goal: Tricking People to give up info.

Generation 4— Approx. 2010, rise of targeted, attacks affected most businesses and drove anti-bot and sandboxing products. Weak out dated software.

Generation 3— Early 2000s, exploiting vulnerabilities in applications affected most businesses and drove intrusion prevention systems (IPS) products.

Generation 2— Mid 1990s, attacks from the internet affected all business and drove creation of the firewall.

Generation 1— Late 1980s, virus attacks on stand-alone PCs affected all businesses and drove anti-virus products.

1990   2000   2010   2017   2020

How are breaches happening?

- 91% of all cyber attacks begin with a **phishing** email to an unexpected victim

- 32% of all successful breaches involve the use of **phishing** techniques

- 147,000 **session token** replay attacks were detected by Microsoft in 2023, a 111% increase year-over-year

- Stealing **session tokens** bypasses authentication controls like MFA

- People + Email

Layers of Cybersecurity

- We implement 35 controls to protect clients and keep them compliant
  - Some are Technical Controls
    - NGAV
    - Zero-Trust
  - Some are Administrative Controls
    - Physical Security
    - Regular Audits
    - Company Policies
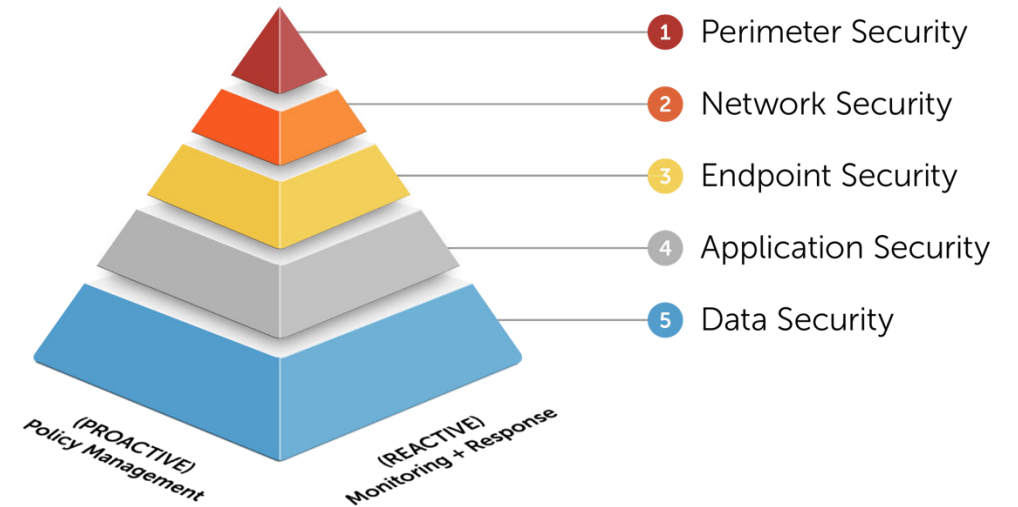
Cybersecurity

What should I do next?

Top 4

- Phishing Training
- Implement Zero-Trust
- MFA/2FA
- Eliminate Saved Sessions

Compliance

- Most Common
  - SOC 2 – SaaS Companies, Cloud Providers
  - ISO 27001 – Very rigorous, 114 controls
  - PCI-DSS – Credit Card requirement
  - FedRAMP – Cloud Service Providers
  - StateRAMP
  - TX-RAMP
  - CMMC – DoD – Comprehensive
  - HITRUST – Health-related organizations
  - ISO/IEC 42001 – AI Systems
  - DORA – European Union

CMMC

CMMC Compliance Domains

Access Control (AC) - All Levels

Awareness & Training (AT) - Level 2, 3

Audit & Accountability (AU) - Level 2, 3

Configuration Management (CM) - Level 2, 3

Identification & Authentication (IA) - All Levels

Incident Response (IR) - Level 2, 3

Maintenance (MA) - Level 2, 3

Media Protection (MP) - All Levels

Personnel Security (PS) - Level 2, 3

Physical Protection (PE) - All Levels

Risk Assessment (RA) - Level 2, 3

Security Assessment (CA) - Level 2, 3

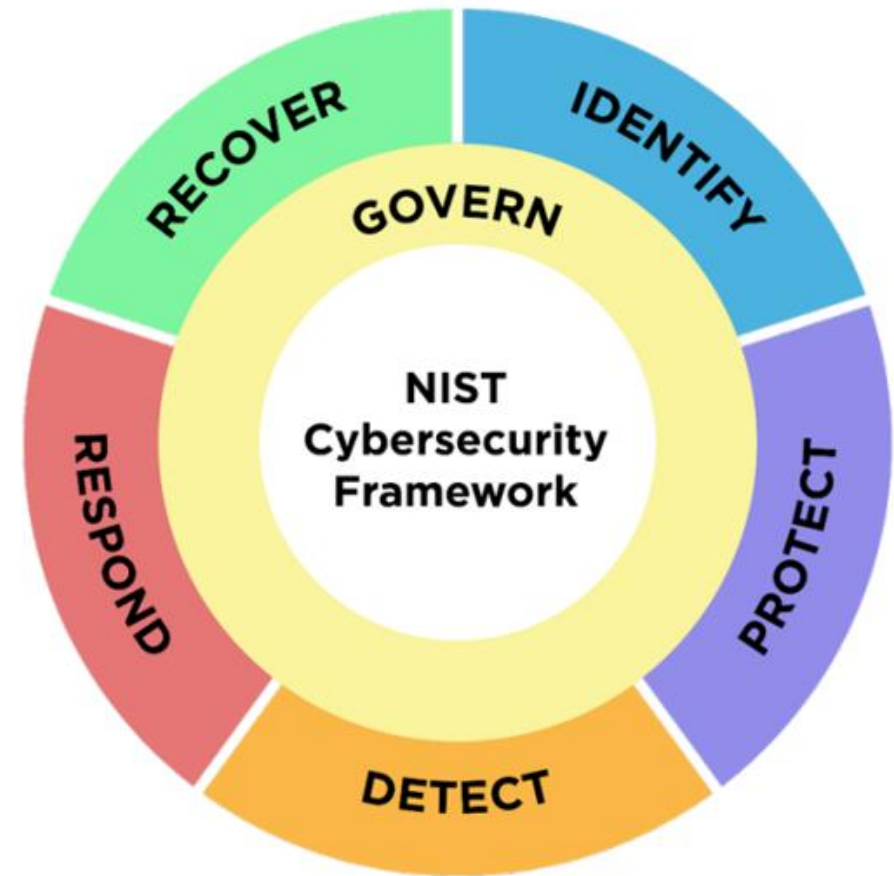System and Communications Protection (SC) - All Levels

System and Information Integrity (SI) - All Levels

Compliance

What should I do next?

NIST CSF 2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

SILICON PLAINS

IT - Cybersecurity - Compliance

Herb Miner
B.S. Computer Systems Engineering
MBA
Co-Founder and Chief Operations Officer
Silicon Plains, LLC

siliconplains.net - 877-287-7762 - herb@siliconplains.net