Port of San Diego
Information Technology

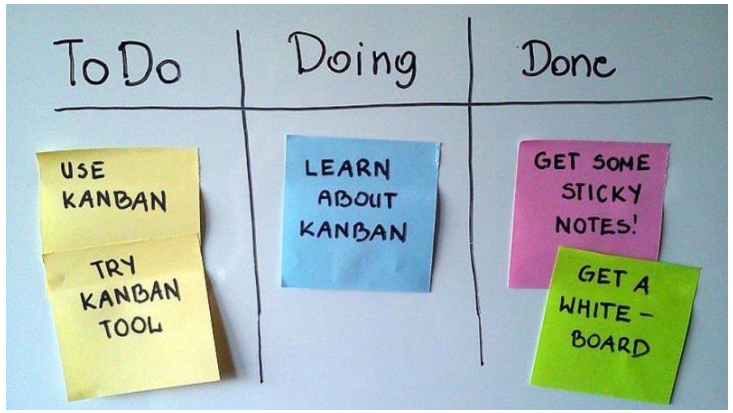
Agenda

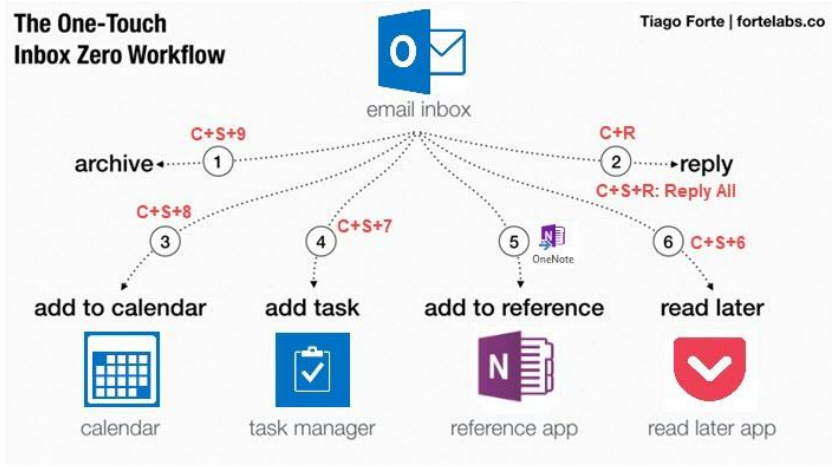
AAPA Executive Conference

1. Enhancing Productivity (and Collaboration)
2. Securing Against Cyber Attacks

Section 1:
Enhancing Productivity (and Collaboration)

Systems to improve productivity





Team productivity tools

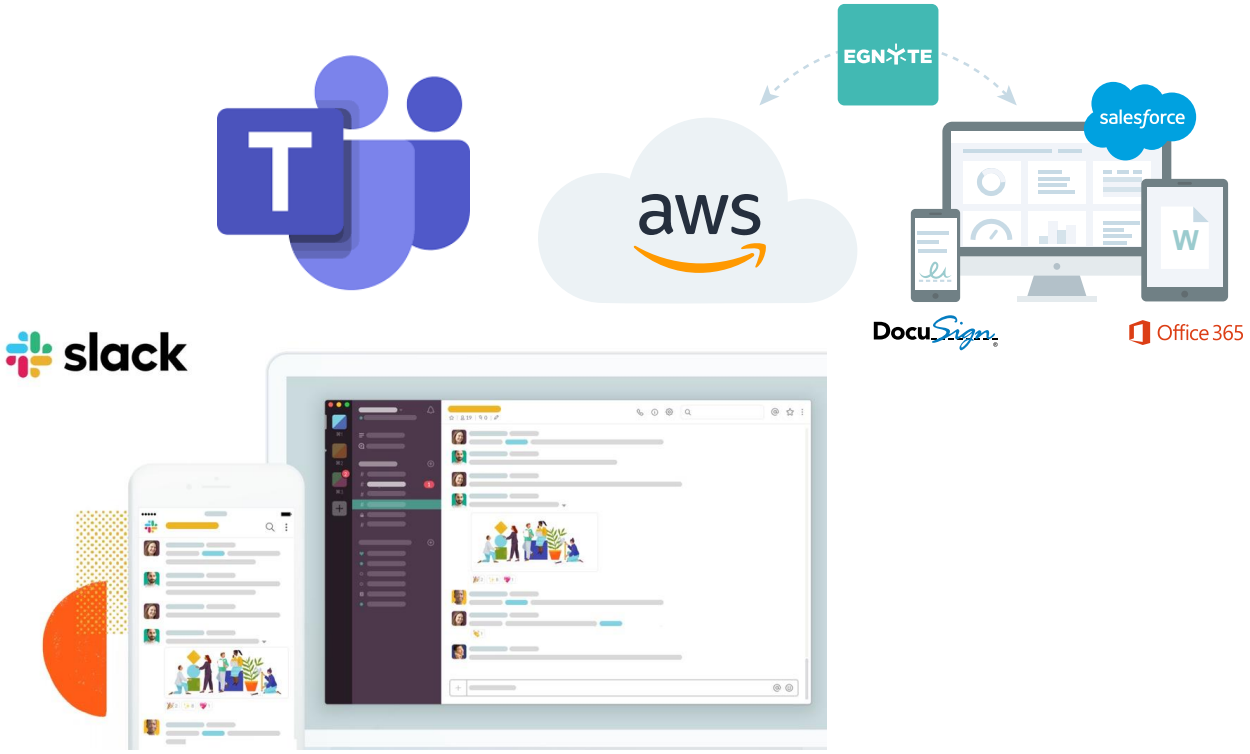
- Social apps in the workplace – Slack, Microsoft Teams, etc.
- Email and Instant Messaging
- Document sharing – SharePoint, DropBox, OneDrive, etc.
- Project Management – Microsoft Project, Asana, etc.
- Task Management – Microsoft Planner, Trello, etc.
- Shared notes – OneNote, Evernote, etc.

The good

Increase collaboration - *Improved communication and collaboration through social technologies could raise the productivity of interaction workers by 20 to 25 percent.*

https://www.mckinsey.com/industries/high-tech/our-insights/the-social-economy

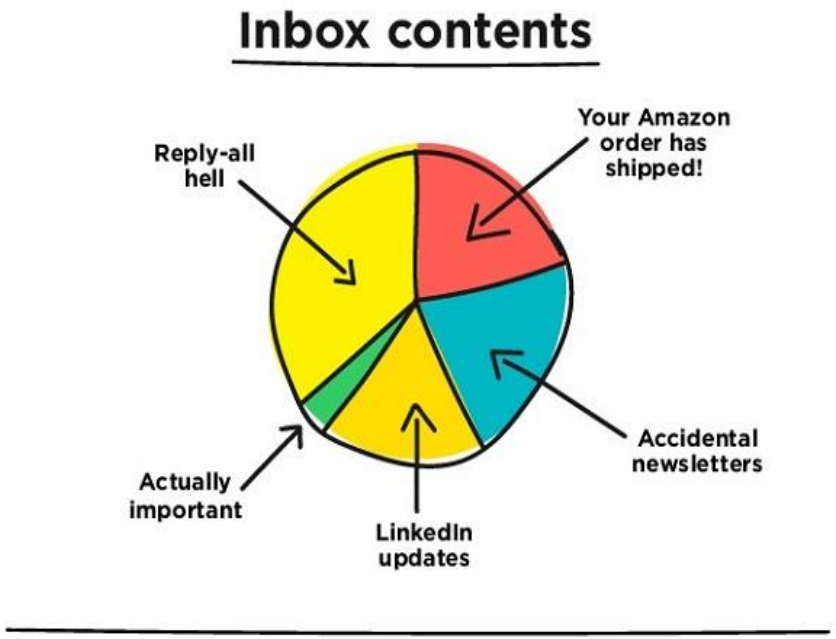
- When used correctly, collaborative apps can boost productivity
- Increase knowledge sharing
- Drive standardization



The bad

The average interaction worker spends an estimated 28 percent of the workweek managing email and nearly 20 percent looking for internal information or tracking down colleagues who can help with specific tasks

https://www.mckinsey.com/industries/high-tech/our-insights/the-social-economy



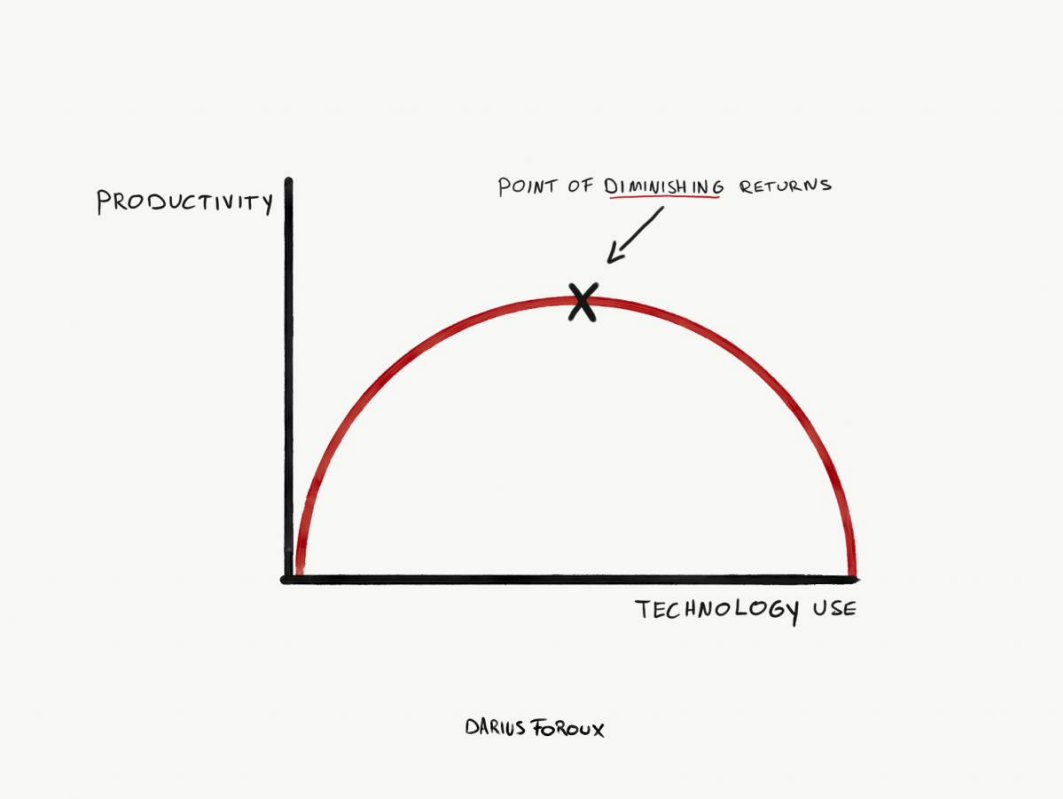
The ugly

Diminishing return of technology – when technology gets in the way of productivity

So, how do we prevent diminishing returns?

Create clear operating procedures for your teams.

- When do you send an email
- When do you message in Slack/Teams
- When do you Instant Message
- When do you create an in person meeting



Don't let the tools and process get in the way

Deliberate communication

Use IM and persistent chat to: reduce emails and voicemails, increase connecting with others asynchronously if they are offline, reduce hallway conversations, increase meeting effectiveness, enable remote workers

Set expectations for you team / organization

- Chat
- Email
- Phone
- Social apps
- Intranet
- Live streaming

Make work visible

Knowledge sharing between shifts and teams

Teamwork

- Enable continuous discussion across teams and vendors
- Create standards and share them online in a secured location
- Streamline project communication
- Status updates
- Bring new team members up to speed quickly

Ways to improve productivity

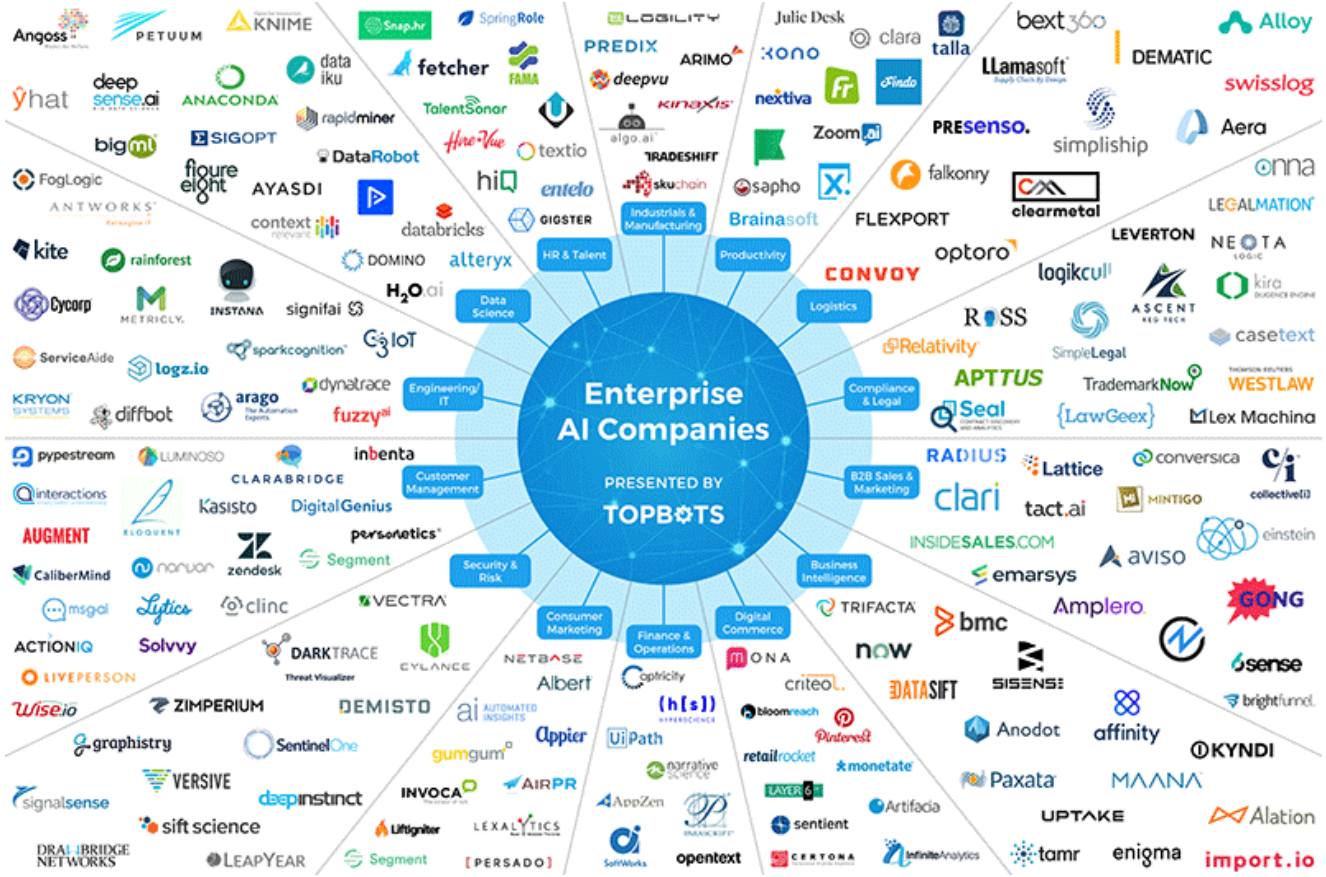
- Create an open and communicative environment
- Connect teams virtually within the company
- Go paperless
- Automate where possible
- Consider that value is more important than cost
- Focus on communication

Future of productivity

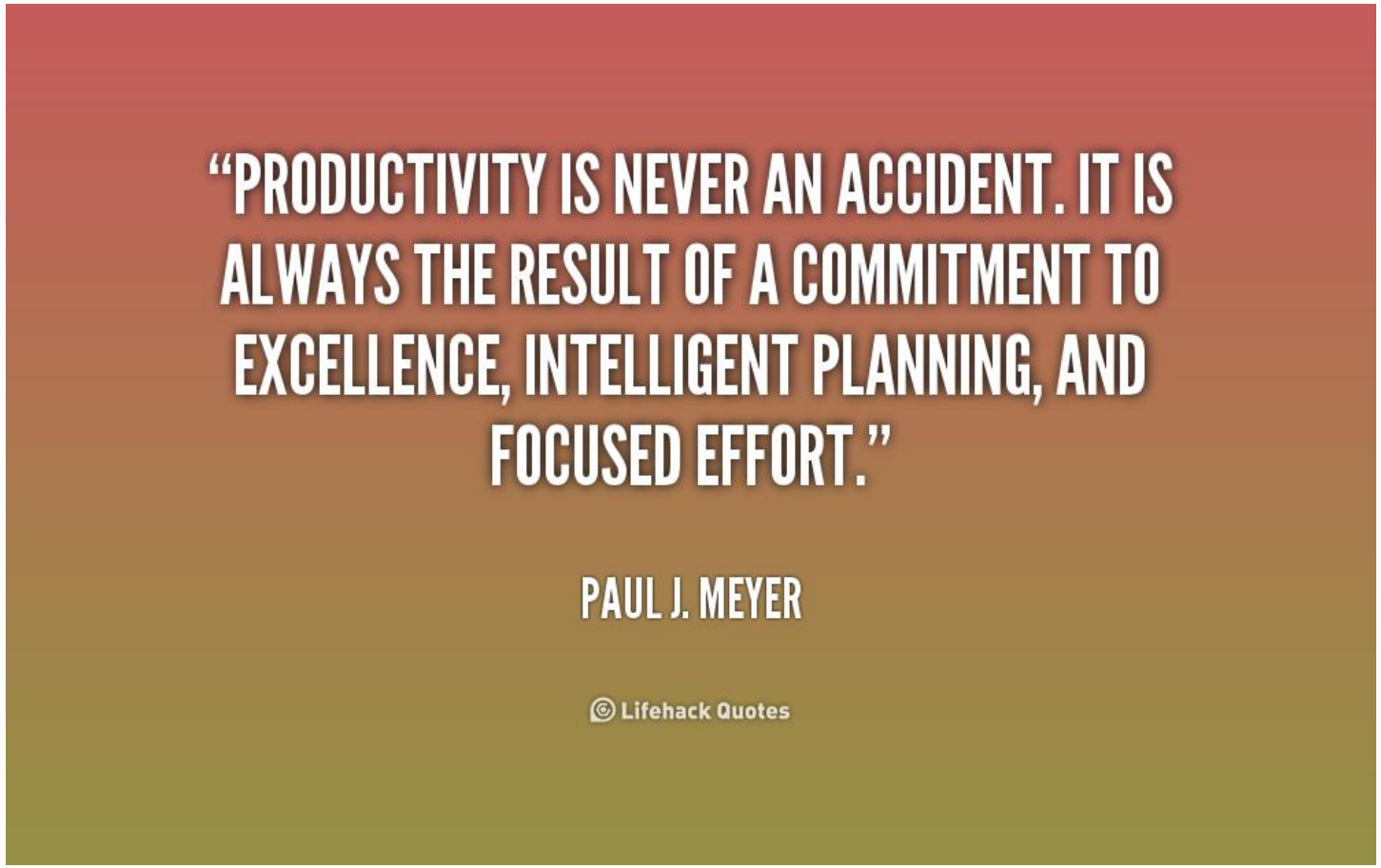
- ChatBots – Open work orders, request board agendas, reserve resources, book meeting rooms, etc.
- Artificial Intelligence – Virtual Assistants
- Machine Learning - revenue projections, expense projections
- Analytics – See how well teams are working together, understand where your time is being spent and stack it against your priorities

Artificial Intelligence / Virtual Assistants

- Schedule meetings
- Find documents
- Book a meeting room
- Notifications of upcoming events or tasks



Technology can only do so much.....



Section 2:
Securing Against Cyber Attacks

What is cybersecurity?

Cybersecurity deals with mitigating **cyberthreats** the systems and technology that companies and organizations use to fulfill their mission…

Cyberthreats are typically anything that can cause damage or loss by exploiting vulnerabilities in an organizations technology

- Unintentional external threats
- Malicious external threats
- Malicious internal threats
- Unintentional internal threats

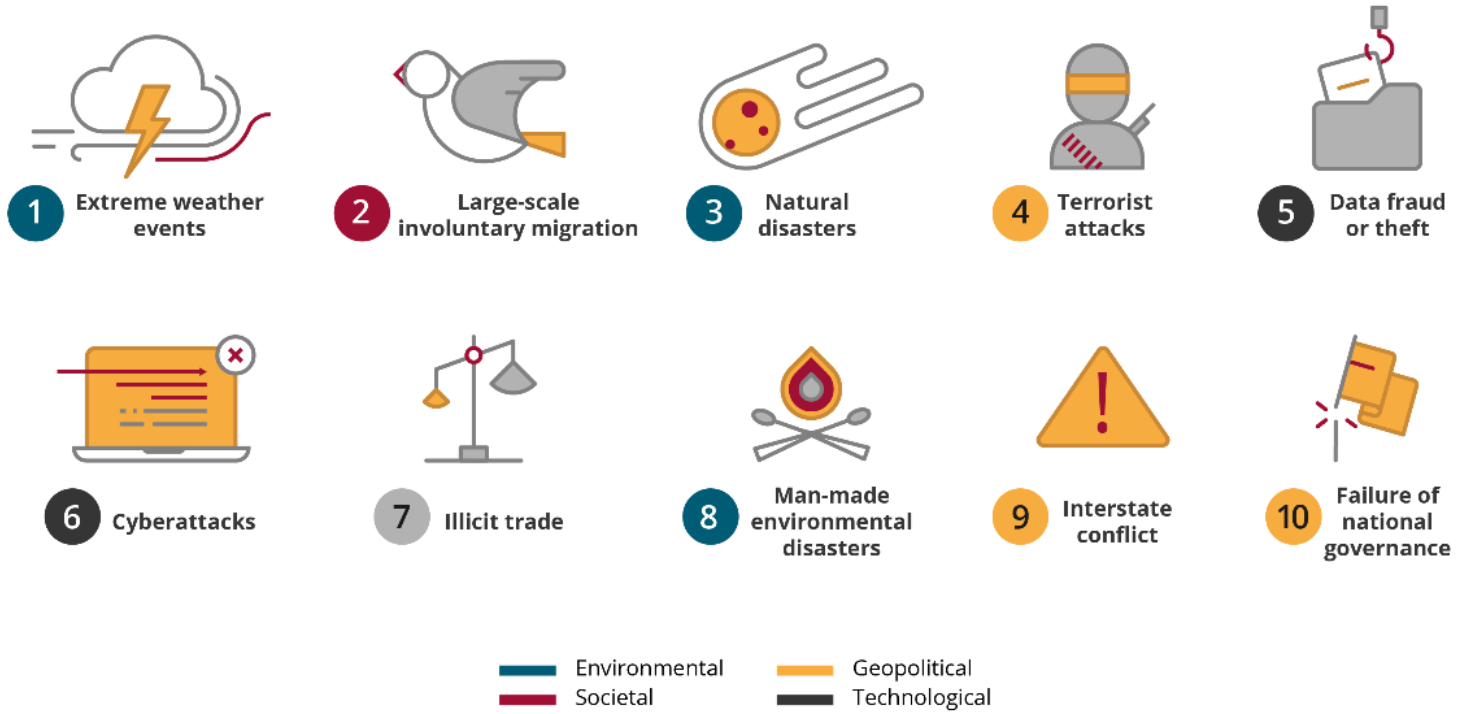
Cyber risks

1. **Business operational risk:** Failure of key business systems, processes, procedures, or people to meet the mission

2. **Reputational risk:** The potential harm caused to an organization's reputation or public image

3. **Legal and compliance risk:** The potential for loss or damage from legal action being taken against an organization for breaching the law or regulatory requirements

Cyber risks are in the top 10 risks



World Economic Forum, 2017

Cyber attack surface – more targets

- Computer, servers, mobile phones and tablets, Bring Your Own Device (BYOD)
- Electronic locks and gates, security cameras
- Thermostats, building automation
- 2020 there will be 50 billion devices connected to IoT
- 70% of IoT devices do not have proper cybersecurity measures in place (Hewlett Packard, 2015)

Mitigating cyber risks

- Use an effective cybersecurity framework
- Make sure responsibilities are known and distributed
- Have a holistic approach to cybersecurity
  - Technical
  - People
- Perform risk assessments on a regular basis
- Have an incident response plan and exercise the plan

Frameworks

Exploring cybersecurity frameworks:

ISO/IEC Security Control Standards**:** Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), specifies an information security management system (ISMS) for managing information risks effectively.

FFIEC Cybersecurity Assessment: Developed by the Federal Financial Institutions Examination Council (FFIEC) to ensure that financial institutions have accurate threat information to protect themselves and their customers from cyberattacks.

SEC/OCIE Cybersecurity Initiative: Developed by the U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) to assess the cybersecurity preparedness of investment firms.

FCC Cyber Security Planning Guide: Developed by the Federal Communications Commission (FCC) to assist small businesses in developing and maintaining policies for protecting critical business data.

NIST Cybersecurity Framework: Created by the National Institute of Standards and Technology (NIST), provides implementation details for managing cybersecurity in the manufacturing environment.

A balanced distribution of responsibility

Every member of the organization: Every member of an organization must have a clearly defined part to play in protecting its critical systems, networks, and data

Executive members: Executives need not become experts in the technicalities of cybersecurity, but it is important to distribute the responsibility for cybersecurity beyond the CIO/CTO team or the chief information security officer (CISO)

Risk committee: Establish a risk committee comprising board members, members from various departments (for example, human resources, physical security, and cybersecurity teams), and members of the executive management team (CEO, CISO, chief risk officer, etc.)

CEO: the CEO sets the tone for cybersecurity by making it an important part of the organizational culture.

Incident Response Plan

- Understand your incident response methodology
- Stakeholders: Who will be involved in incident response? This can span from IT to security, legal to HR, to an executive sponsor
- Know your roles and responsibilities: Who is in the lead?
- All contact information for each involved primary and secondary stakeholder is recorded
- Know how you will work the incident
- What defines an incident? Define it before it happens
- Define a Critical, High, Medium, and Low severity incident
- Map out your workflow and process
- Make sure you have any vendors you will need on retainer
- Practice your Incident Response Plan

Port specific

Critical Infrastructure

- Potentially targeted by nation states
- More advanced mitigating technics required

Resilience

- Have the ability to bounce back

Network Segmentation

- Protect the most important assets
- SCADA systems are at risk and should be segmented off

Active defense

- Hunt teams – don’t just trust tools to passively look for evidence of attacks

Securing against cyber attacks

Can we really secure against attacks?

You really can’t secure 100%

“The adage is true that the security systems have to win every time, the attacker only has to win once.”

Dustin Dykes, CISSP

Founder Wirefall Consulting

Be prepared!

Cyber events will happen…the biggest risk is to pretend the risks don’t exist…

Risk mitigation and incident planning will enabled you to deal with what comes

Thank you!

PORT of SAN DIEGO
Waterfront of Opportunity