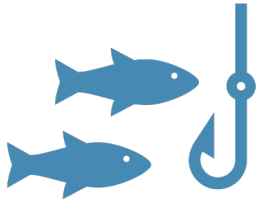
The Flagship Security Framework

Preventing Costly Attacks and Providing Peace of Mind

Typical Security Threats

Dark Web Threats



Phishing Scams

Email Attachments

Inside Bad Actors

External Vulnerabilities

Attacks on SaaS Solutions

FLAGSHIP

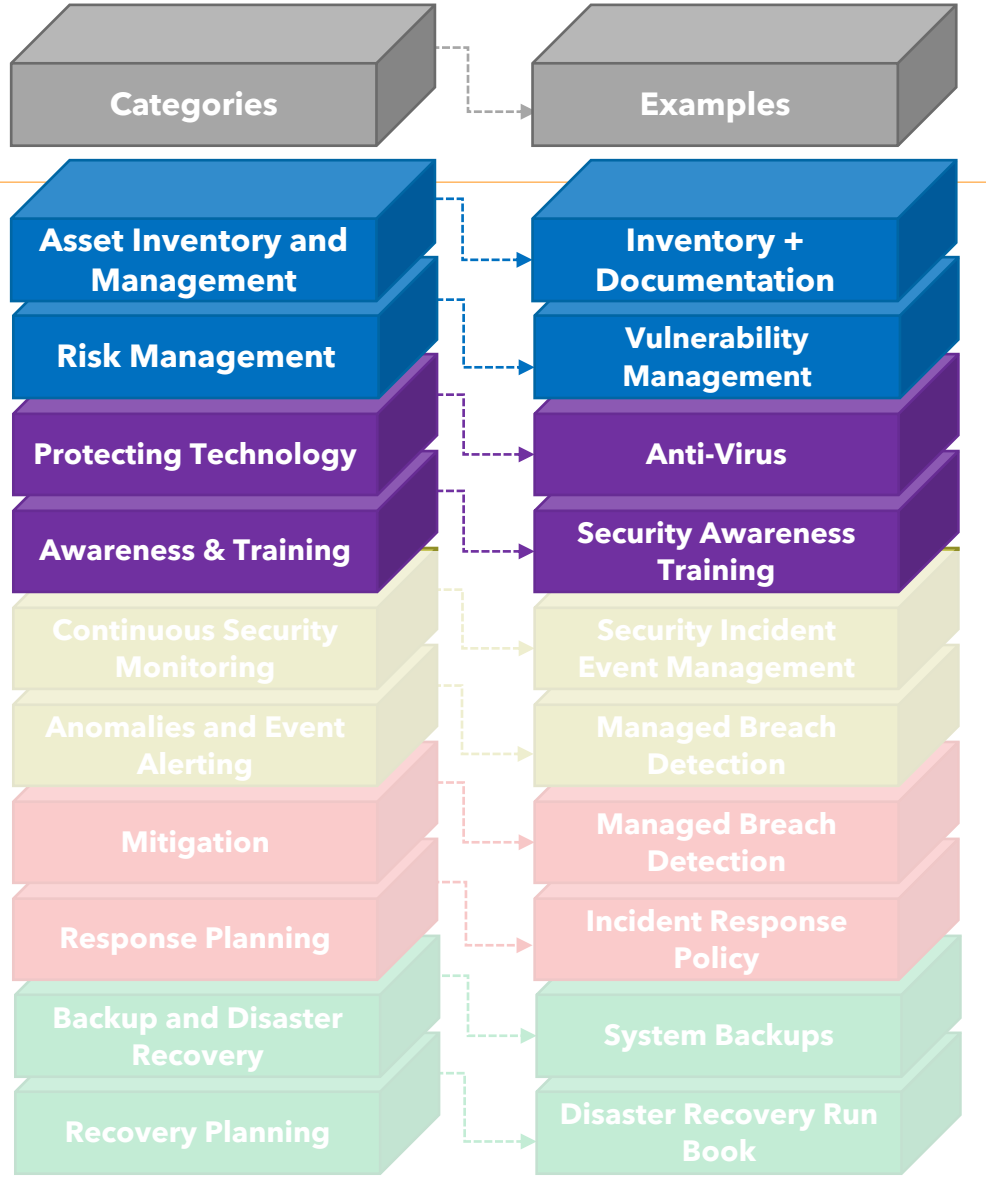
Flagship Security Framework & SecOps Team

FLAGSHIP

Framework Functions

Develop the organizational understanding to manage risk to systems, assets, data, and capabilities. Identify revolves around pinpointing all the systems and platforms included in the company's infrastructure.

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Protect calls for limiting and controlling secure access to essential systems and physical and digital assets, as well as putting protections in place to prevent any unauthorized access.

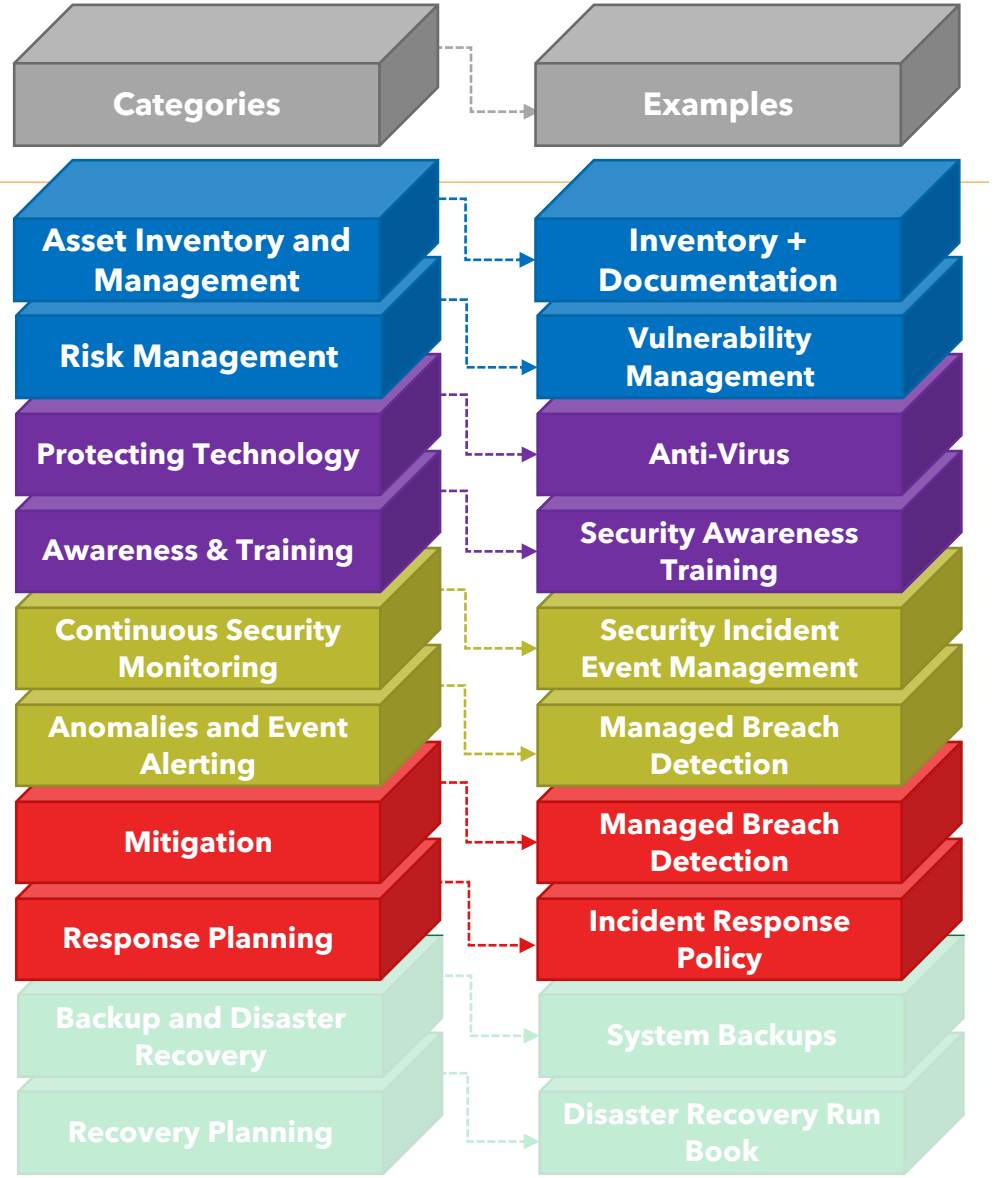


FLAGSHIP

Framework Functions

Detect develops and implements the appropriate activities to identify the occurrence of a security event. The Detect Function enables timely discovery of cybersecurity events to ensure that the effects of the event can be minimized.

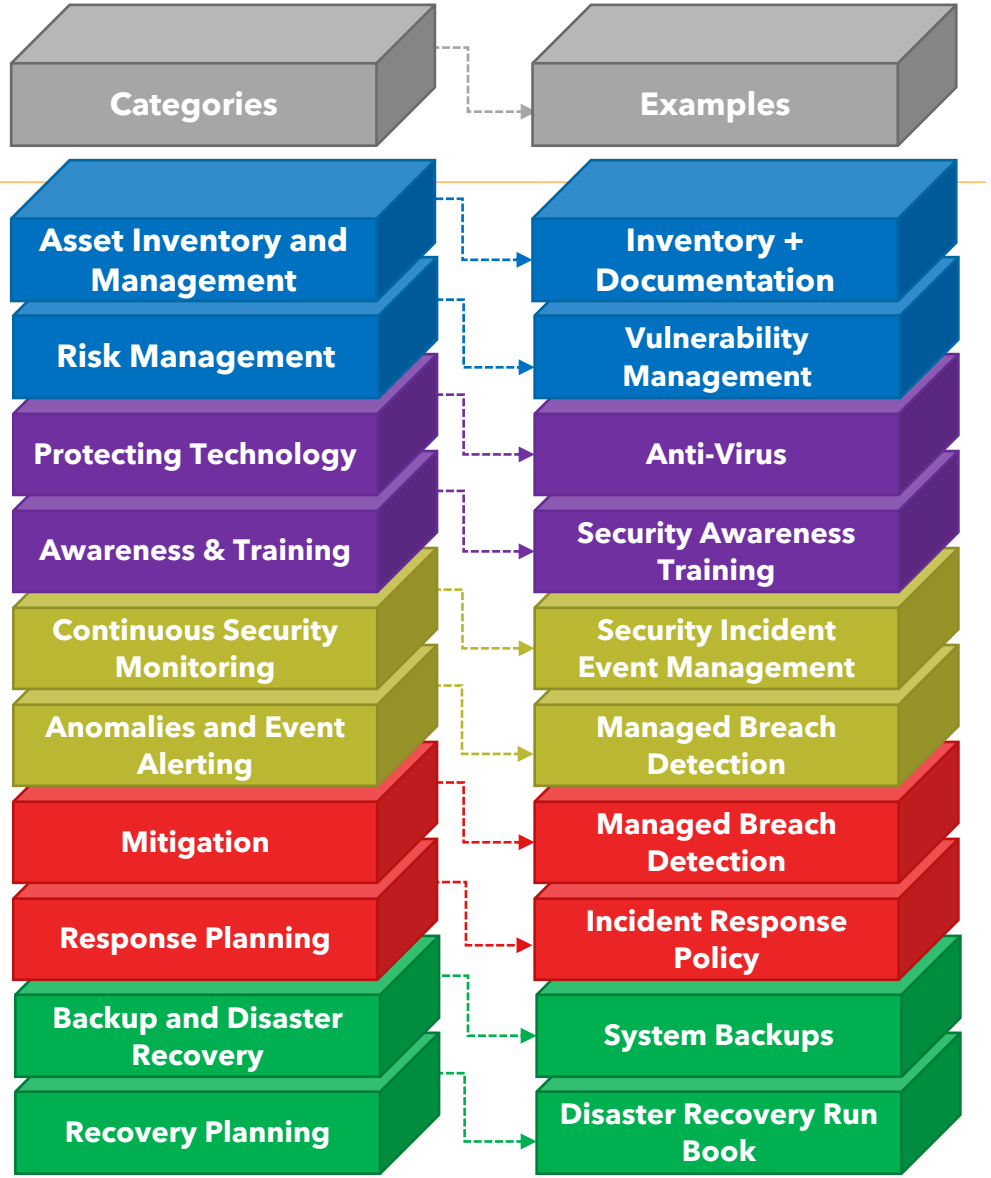
Respond develops and implements the appropriate activities when facing a detected security event. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident, limiting service interruptions and/or potential stolen data.



FLAGSHIP

Framework Functions

Recover develops and implements the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a security event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.



FLAGSHIP

Framework Tracks

The **Security Framework** further defines the National Institute of Standards and Technology (NIST) Cyber Security Framework by specifying **Tracks** within an organization's IT system. The four tracks assist with pinpointing the weakest areas.

- **Users**
- **Endpoints**
- **Infrastructure**
- **Network**

The tracks greatly assist with managing risk by ensuring all aspects of the environment are covered.

FLAGSHIP

Sample Protection Layers: Basics

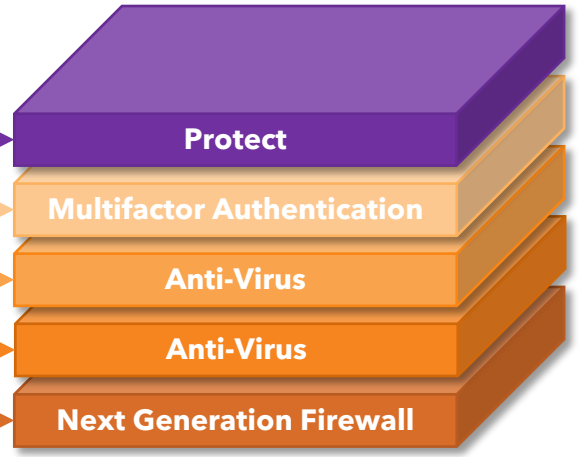
Protect your assets → Identity Management & Access Control, Awareness & Training, Protecting Technology

Users identity & acess → User Identity, Access Control, Authentication. & Policies.

Enpoints workstations & phones → Workstations, Laptops, Phones, Tablets and other IoT.

Infrastructure servers & applications → Servers, SaaS and Applications.

Network firewall & switches → Switches, Routers, Wireless & Firewalls.



FLAGSHIP

Sample Protection Layers: Next Steps

Protect your assets → Identity Management & Access Control, Awareness & Training, Protecting Technology

Users identity & acess → User Identity, Access Control, Authentication. & Policies.

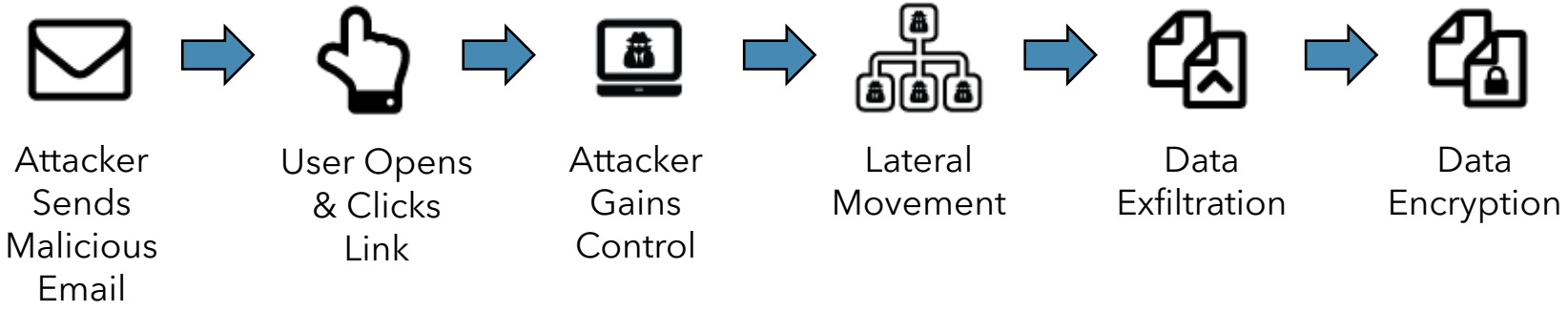
Enpoints workstations & phones → Workstations, Laptops, Phones, Tablets and other IoT.

Infrastructure servers & applications → Servers, SaaS and Applications.

Network firewall & switches → Switches, Routers, Wireless & Firewalls.

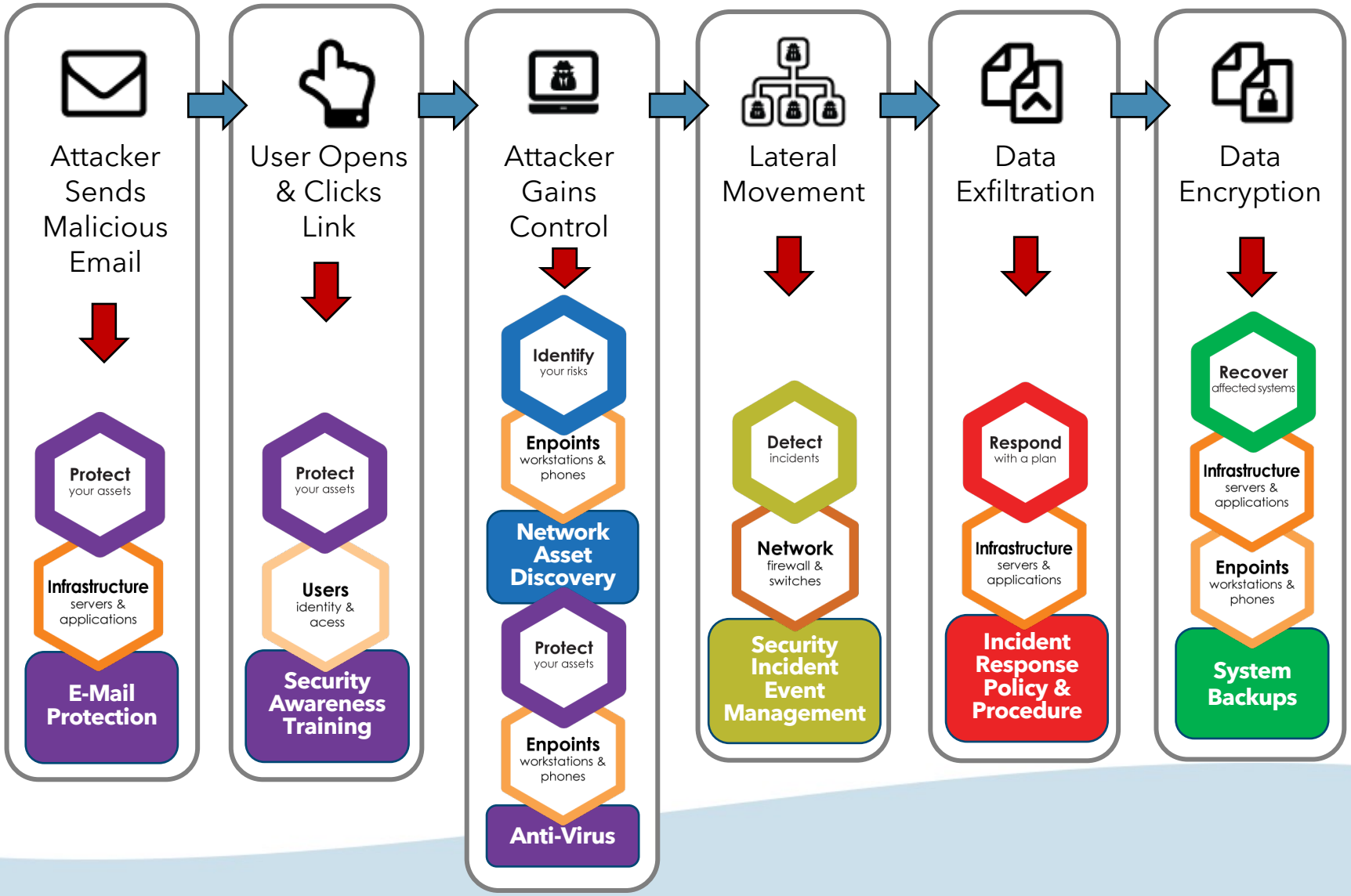
FLAGSHIP

Case Study: Attack on a Manufacturer



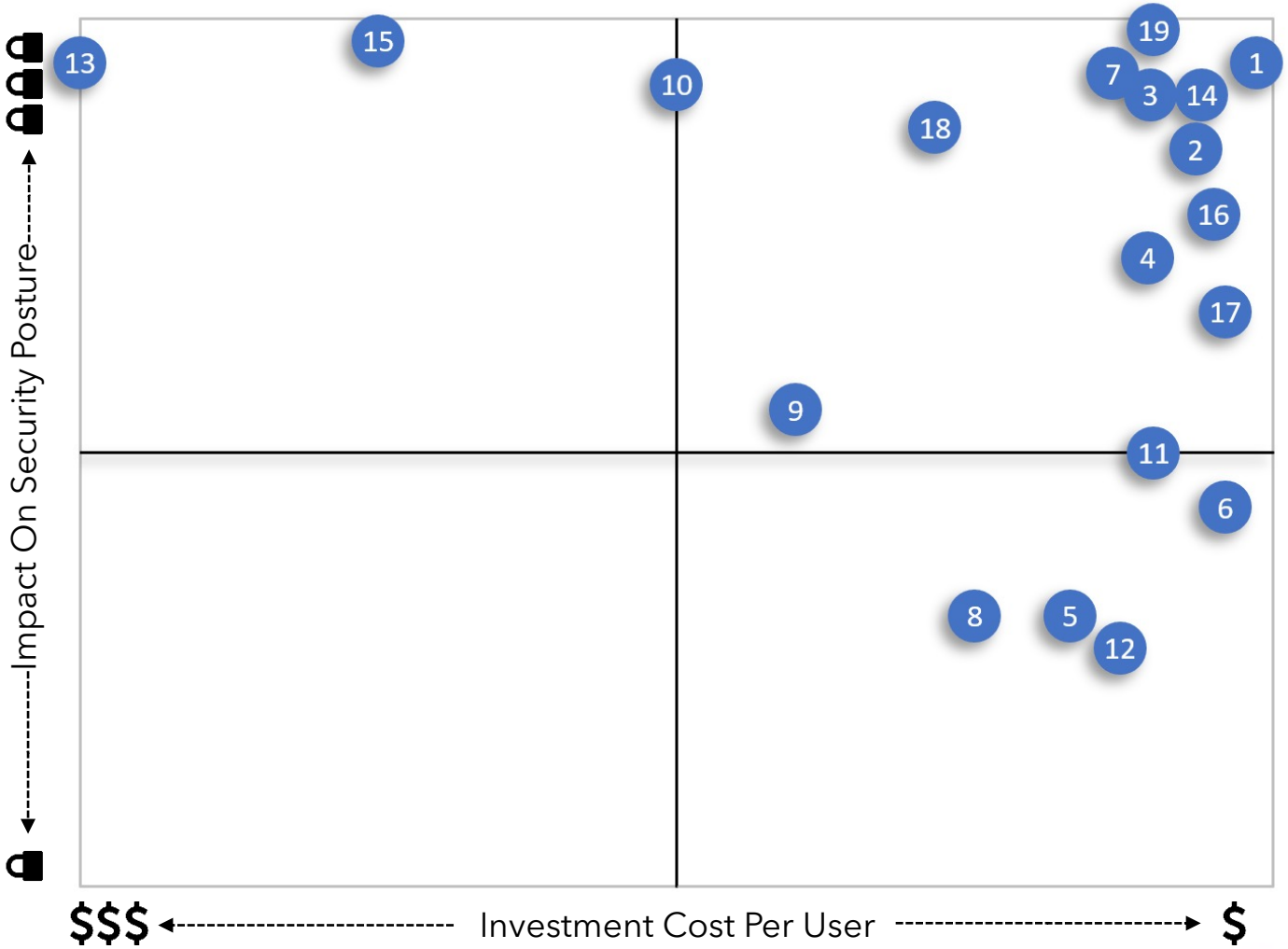
FLAGSHIP

Case Study: Recovery and Prevention



FLAGSHIP

Impact vs. Investment



1 **Enforced Password & Lockout Policy**
2 **Standard Endpoint Protection**
3 **Advanced Endpoint Protection**
4 **Next-Gen Firewall**
5 Network Segmentation
6 Standard E-Mail Protection
7 **Advanced E-Mail Protection**
8 Cybersecurity Insurance
9 **Vulnerability Management**
10 Data Backups
11 Dark Web Monitoring
12 Disk Encryption
13 Security Incident Event Management
14 **Managed Breach Detection**
15 Offsite Data Backups
16 **Security Awareness Training**
17 Phishing Campaign
18 **Disaster Recovery Run Book**
19 **Multi-Factor Authentication**

FLAGSHIP

Your Next Steps

1. Complete a security assessment
2. Define your objectives
3. Build your security roadmap.

FLAGSHIP