Security Incidents & Root Causes Report

PREPARED FOR:

Mike Buma
Info-Tech Research Group

January 26, 2015

IT SECURITY DIAGNOSTIC PROGRAM
POWERED BY INFO-TECH RESEARCH GROUP

INFO~TECH RESEARCH GROUP

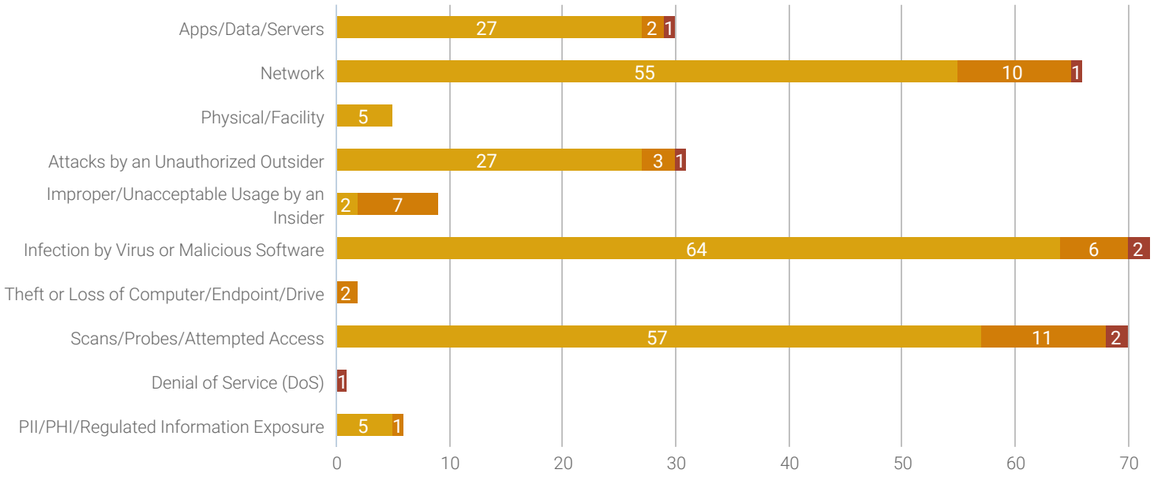
Incidents and Root Causes Summary

Minor Incidents | Major Incidents | Critical Incidents

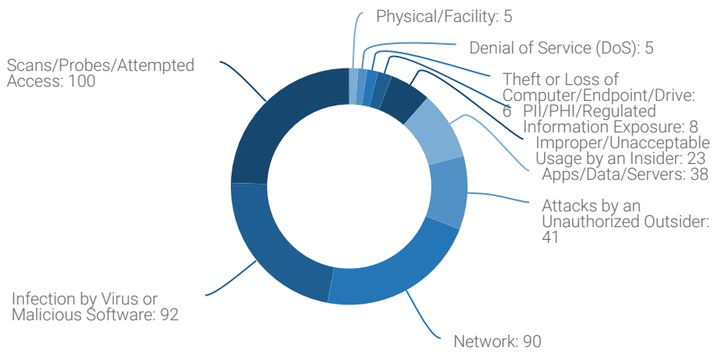
Security Incidents

Please indicate the number of actual security incidents (network breach, data loss, etc.) that have occured in these areas during this time period.

of Incidents



Weighted by Severity



Critical = x5 | Major = x3 | Minor = x1

Top Incident Areas:

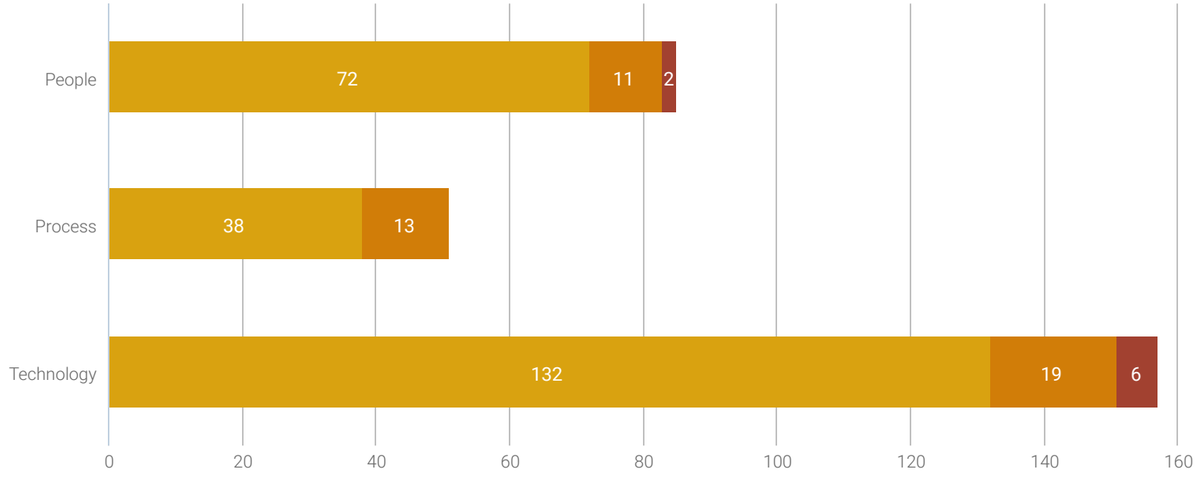
Infection by Virus or Malicious Software (highest # of incidents)

Scans/Probes/Attempted Access (highest weighted score)

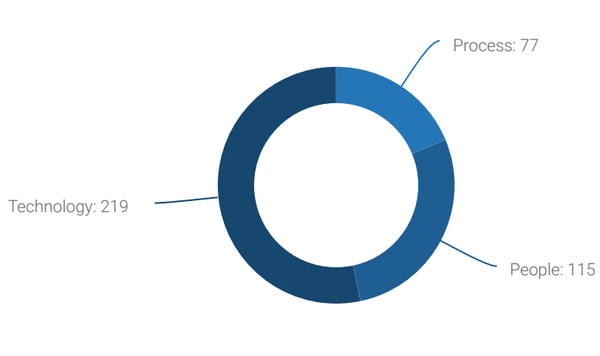
Root Causes

Please indicate the root causes for incidents experience in these areas during this time period.

of Incidents



Weighted by Severity



Critical = x5 | Major = x3 | Minor = x1

Top Root Causes:

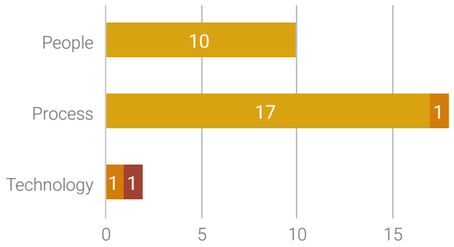
Technology (highest # of incidents, and weighted score)

Root Causes by Security Area

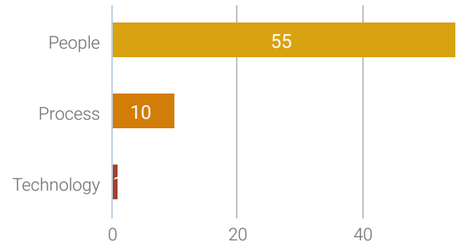
Please indicate the root causes for incidents experience in these areas during this time period.

Minor Incidents Major Incidents Critical Incidents

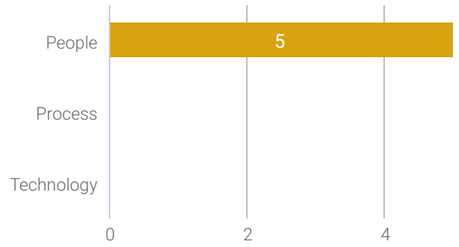
Apps/Data/Servers



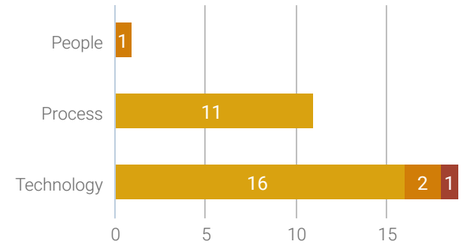
Network



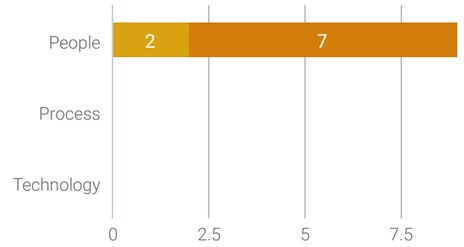
Physical/Facility



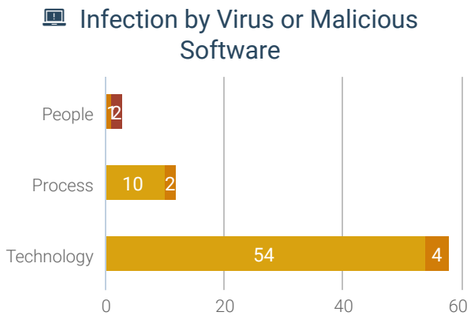
Attacks by an Unauthorized Outsider



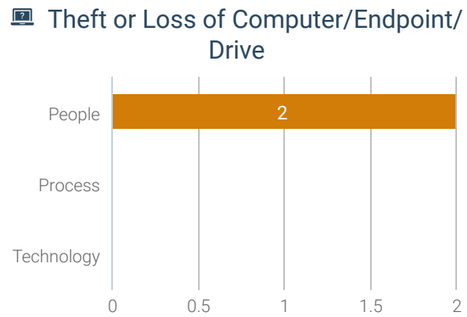
Improper/Unacceptable Usage by an Insider



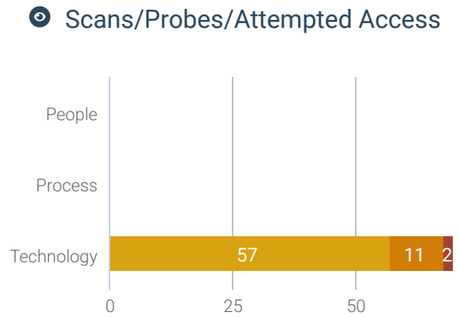
Infection by Virus or Malicious Software



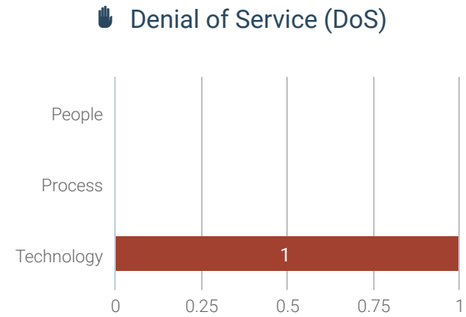
Theft or Loss of Computer/Endpoint/ Drive



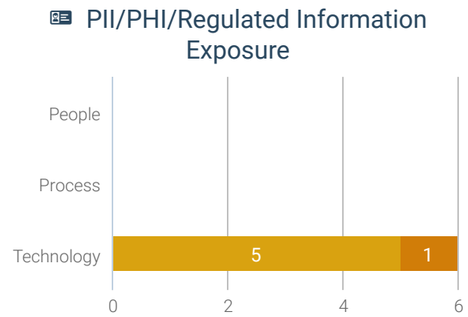
Scans/Probes/Attempted Access



Denial of Service (DoS)

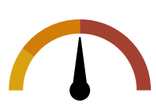
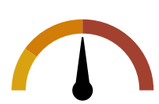
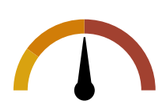


PII/PHI/Regulated Information Exposure



Risk and Impact of Potential Future Incidents

Low Priority Moderate Priority High Prioirty

	Apps / Data / Servers	Network	Physical / Facility	Attacks by an Unauthorized Outsider	Improper / Unacceptable Usage by an Insider	Infection by virus or Malicious Software	Theft or Loss of Computer / Endpoint / Drive	Scans / Probes / Attempted Access	Denial of Service (DoS)	PII /PHI / Regulated Information Exposure
Risk of Incidents:										
Business Impact:										
Combined risk and business impact score:	Moderate	High	Low	High	Moderate	Moderate	High	High	Moderate	High

Overall Trends

2014-09-01 (P1) 2015-01-01 (P2)

Incident Trends

Critical

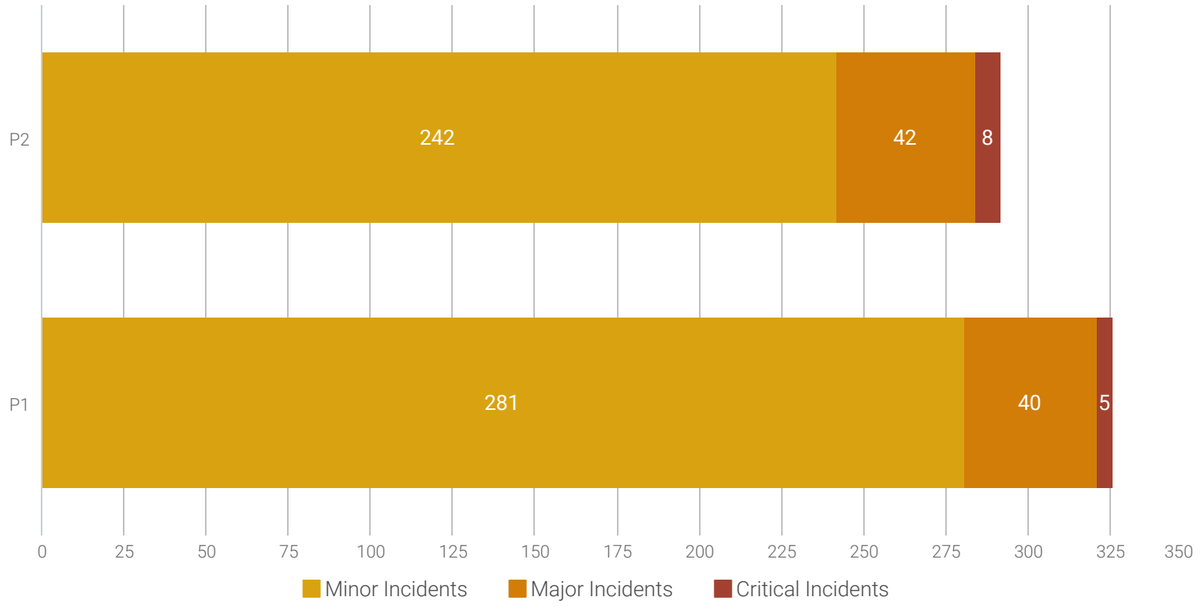
60%
increase

Major

5%
increase

Minor

13%
decrease



Root Cause Trends

People

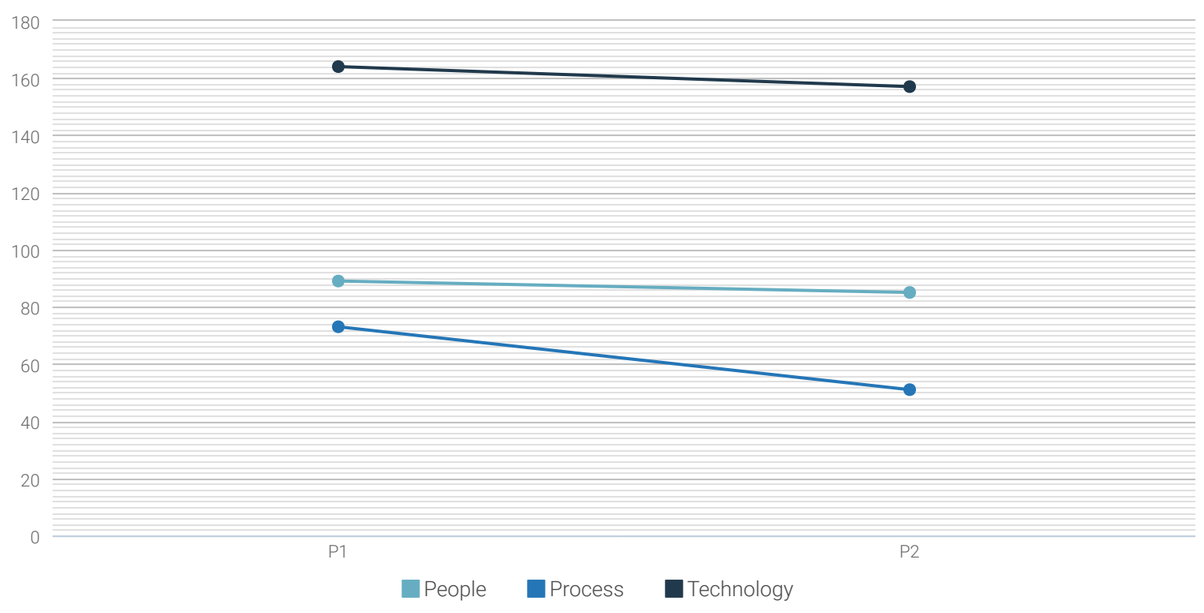
4%
decrease

Process

30%
decrease

Technology

4%
decrease



Security Incidents and Root Causes – 2015-01-01 - 2015-04-30

Info-Tech Research Group

Prepared for:
Mike Buma

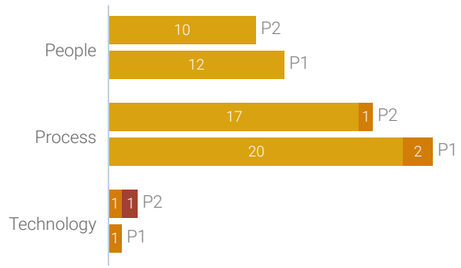
powered by INFO~TECH RESEARCH GROUP

Trends by Security Area

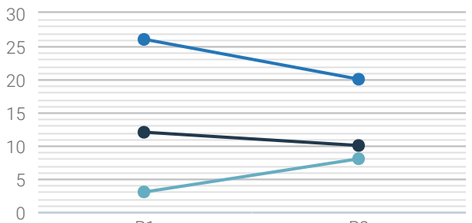
Minor Incidents | Major Incidents | Critical Incidents

People | Process | Technology

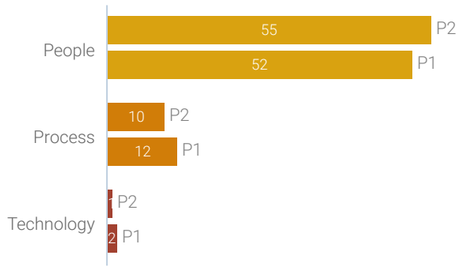
Apps/Data/Servers



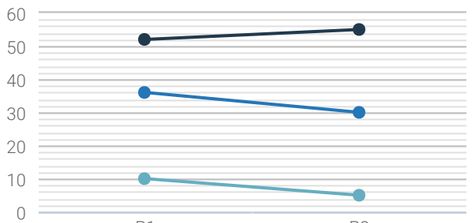
Weighted by Severity



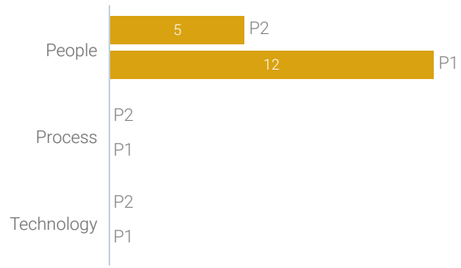
Network



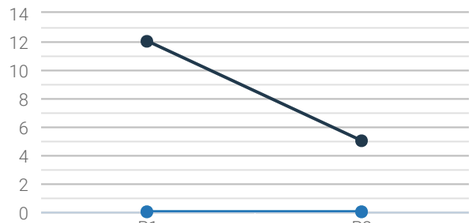
Weighted by Severity



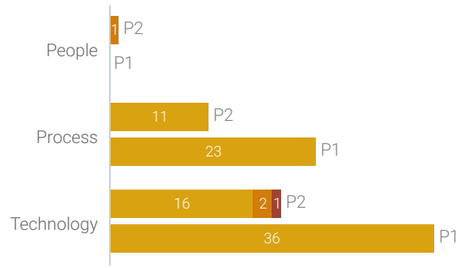
Physical/Facility



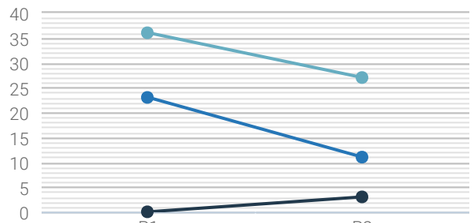
Weighted by Severity



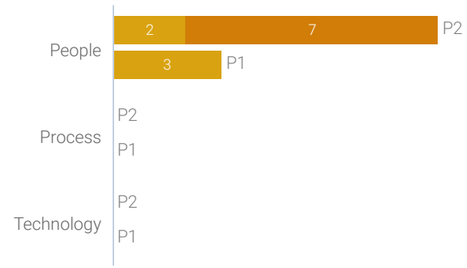
Attacks by an Unauthorized Outsider



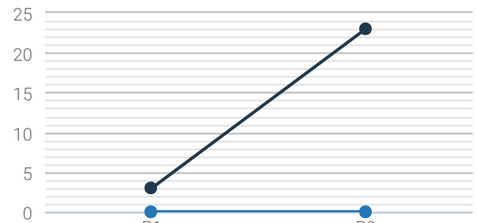
Weighted by Severity



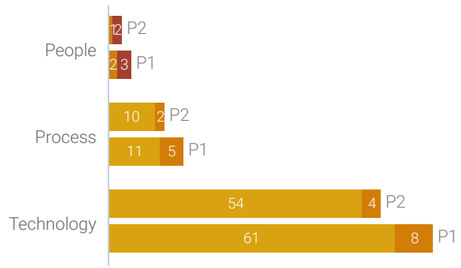
Improper/Unacceptable Usage by an Insider



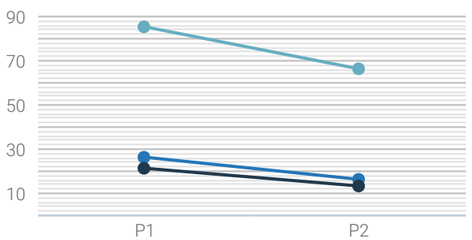
Weighted by Severity



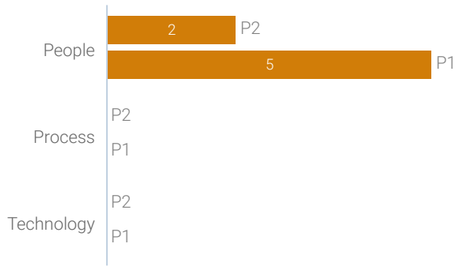
Infection by Virus or Malicious Software



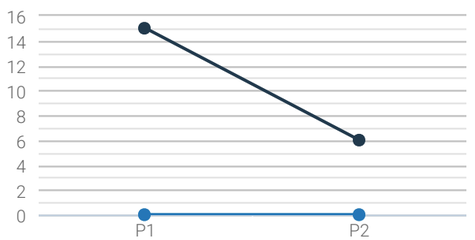
Weighted by Severity



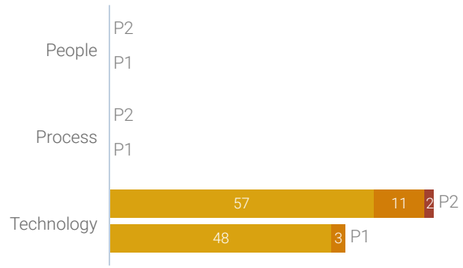
Theft or Loss of Computer/ Endpoint/Drive



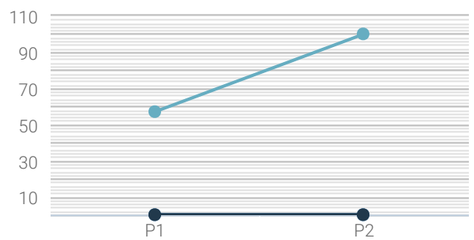
Weighted by Severity



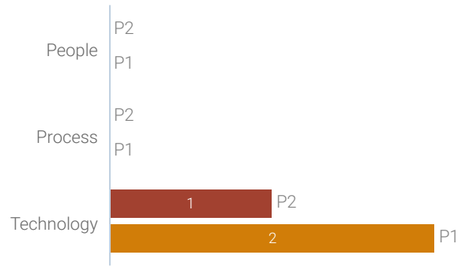
Scans/Probes/Attempted Access



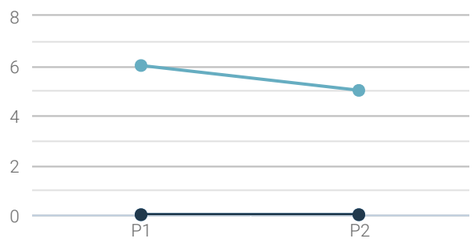
Weighted by Severity



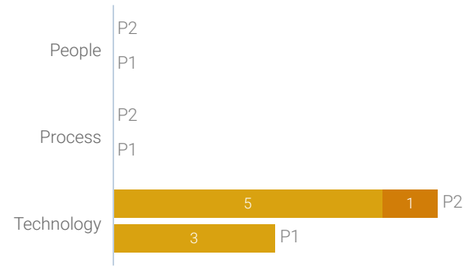
Denial of Service (DoS)



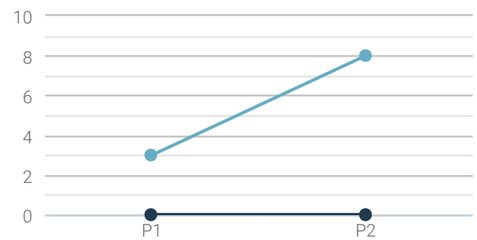
Weighted by Severity



PII/PHI/Regulated Information Exposure



Weighted by Severity



Glossary

Apps/Data/Servers

Any application or server compromise that results in the exposure of data or compromise of the host.

Network

Any attack against the confidentiality, integrity, or availability of the network itself, distinct from attacks that simply leverage network connectivity.

Physical/Facility

Any compromise of the physical security of the facility resulting in potential or actual loss of information.

Attacks by an Unauthorized Outsider

Any attack perpetrated by an individual without legitimate access to internal systems.

Improper/Unacceptable Usage by an Insider

Any incident resulting from inappropriate (contrary to policy) activity by an authorized system user.

Infection by viruses or malicious software

Any incident resulting in the presence of a virus or other malware on an endpoint, server, or other system.

Theft or Loss of Computer/Endpoint/Drive

Any incident resulting in the loss of a, typically end-user, computing asset.

Scans/Probes/Attempted Access

Any network-based attempt to identify system vulnerabilities as a first step to a compromise.

Denial of Service (DoS)

Any attempt to render systems or networks unavailable to legitimate users.

PII/PHI/Regulated Information Exposure

Any loss of personally identifiable, protected health , or otherwise regulated information.