A deep dive into the R+R of the NIST Cyber Security Framework

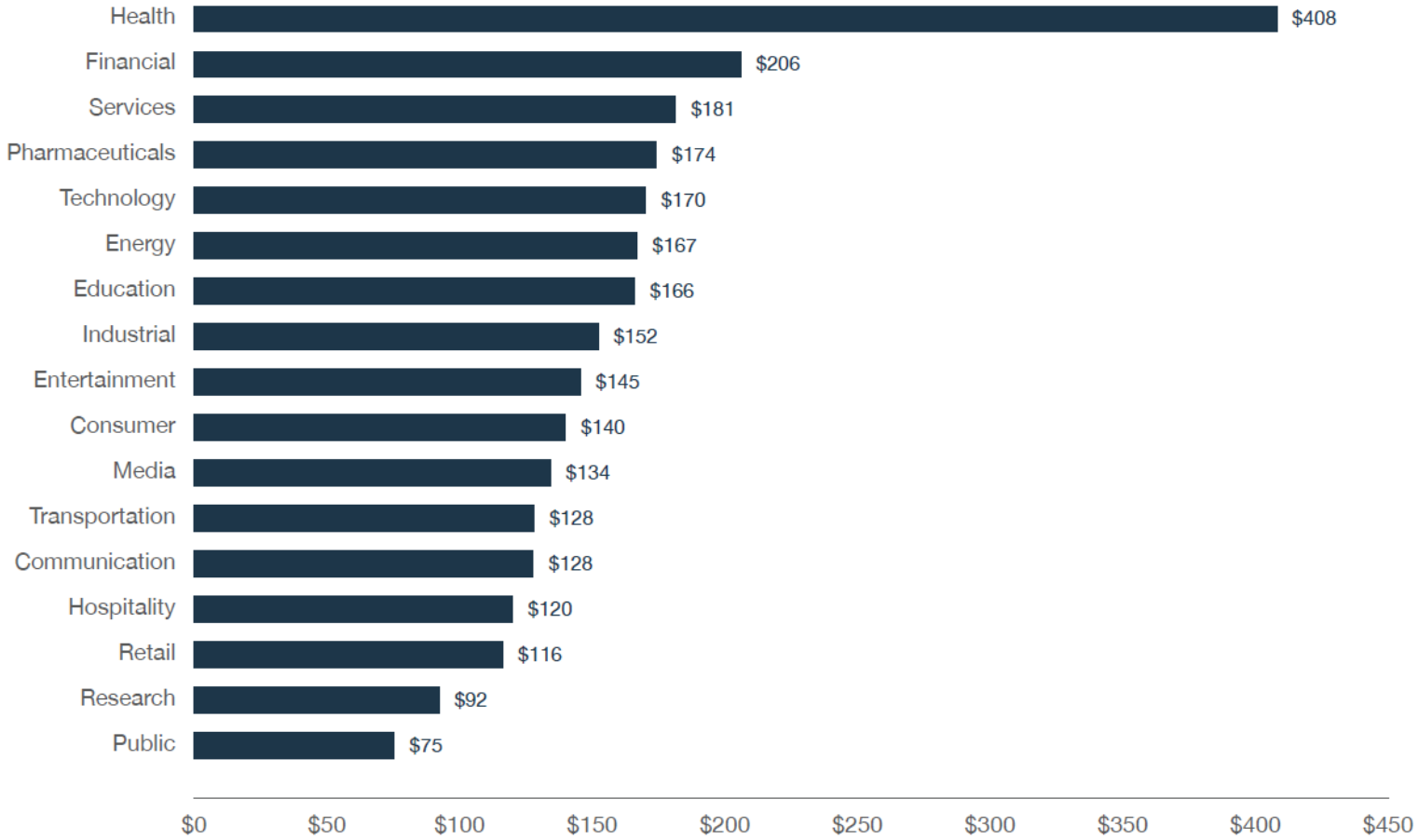
hA Security Champions
June 2019

Incident Response
FORENSIC & CYBER

Case Studies

Figure 7. Per capita cost by industry sector

Measured in US$



NIST


RECOVER
IDENTIFY
RESPOND
CYBERSECURITY
FRAMEWORK
VERSION 1.1
PROTECT
DETECT

Respond


RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
PROTECT
RESPOND
DETECT

Response Planning

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Response plan is executed during or after an incident

Communications

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Personnel know their roles and order of operations when a response is needed

Incidents are reported consistent with established criteria

Information is shared consistent with response plans

Coordination with stakeholders occurs consistent with response plans

Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Analysis

Analysis is conducted to ensure effective response and support recovery activities.

Notifications from detection systems are investigated

The impact of the incident is understood

Forensics are performed

Incidents are categorised consistent with response plans

Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

Incidents are contained

Incidents are mitigated

Newly identified vulnerabilities are mitigated or documented as accepted risks

Improvements

Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Response plans incorporate lessons learned

Response strategies are updated

Recover


RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY
FRAMEWORK
VERSION 1.1

Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Recovery plan is executed during or after a cybersecurity incident

Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Recovery plans incorporate lessons learned

Recovery strategies are updated

Communications

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

Public relations are managed

Reputation is repaired after an incident

Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

INCIDENT RESPONSE SOLUTIONS

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents

Campbell McKenzie
+64 21 779 310 or 0800 WITNESS
campbell@incidentresponse.co.nz
https://incidentresponse.co.nz