2014 DATA BREACH INVESTIGATIONS REPORT

Safeguarding Health Information: Building Assurance through HIPAA Security – 2014

September 23, 2014

verizon

Incidents that 50 global contributors investigated form the basis of the research

Mishcon de Reya

United States Secret Service

KASPERSKY lab

McAfee
An Intel Company

Defense Security Service United States of America

National Cyber Security Centre
Ministry of Security and Justice

European Cybercrime Centre
EC3
EUROPOL

Akamai

G-C PARTNERS

CENTRIPETAL NETWORKS

CIRCL
Computer Incident Response Center Luxembourg

OpenCERT Canada
semper vigilantem

Deloitte.

U.S. Department of Homeland Security
Homeland Security

MALICIOUS STREAMS

GDT
GRUPO DE DELITOS TELEMÁTICOS

S21sec
Comprometidos con la seguridad

REN-ISAC

República de Colombia Policía Nacional
Dios y Patria

AFP
AUSTRALIAN FEDERAL POLICE

POLITI

verizon

ES ISAC
Electricity Sector Information Sharing Analysis Center

CENTER FOR INTERNET SECURITY®

CENTER FOR CYBERSIKKERHED
FE

PT-ISAC

ThreatGRID
Malware Analysis & Threat Intelligence

WINSTON & STRAWN LLP

IRISS
Irish Reporting and Information Security Service

Real Estate ISAC
Information Sharing and Analysis Center

Guidance SOFTWARE
EnCase

CERT.PT

ERT

computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

POLITIE

CERT
Software Engineering Institute
Carnegie Mellon.

WhiteHat SECURITY

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

POLICIA METROPOLITANA

CyberSecurity MALAYSIA
An agency under MOSTI

itrc
Identity Theft Resource Center

FireEye™

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

V C D B

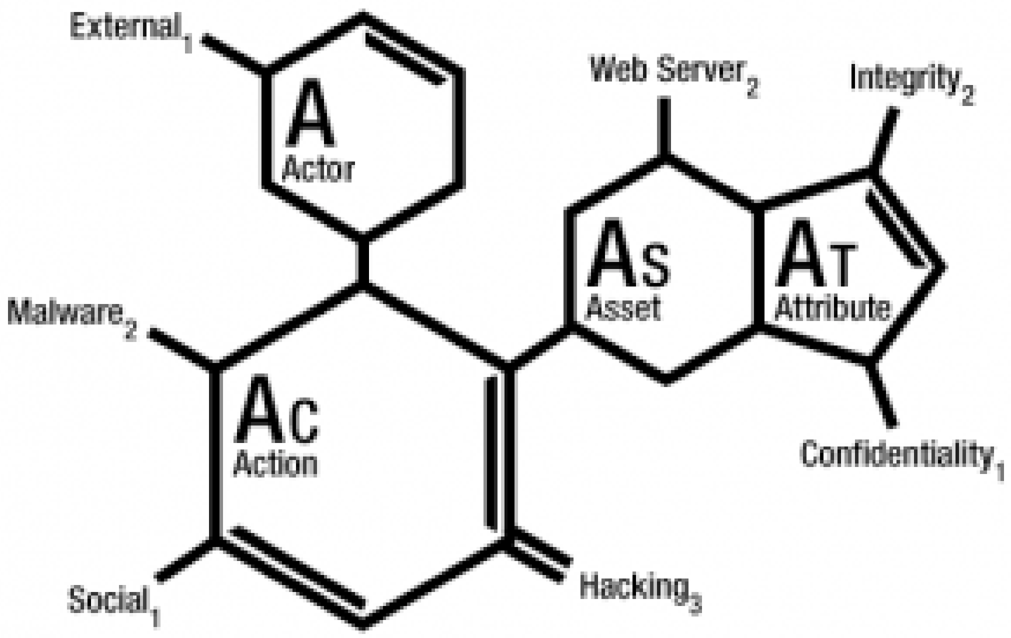
CERT.PL>_

FINANCIAL SERVICES
Information Sharing and Analysis Center

ThreatSim™

Sigillum Reipublicæ Massachusettensis

The DBIR uses the VERIS framework for data collection and analysis



Actor – Who did it?

Action – How’d they do it?

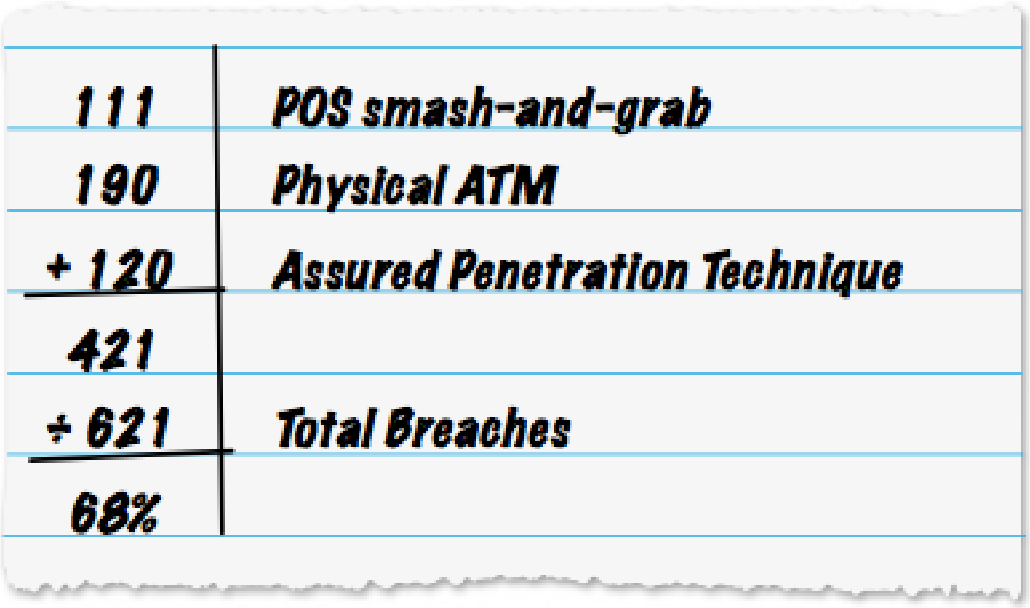
Asset – What was affected?

Attribute – How was it affected?

Documentation, classification examples, enumerations: http://veriscommunity.net/

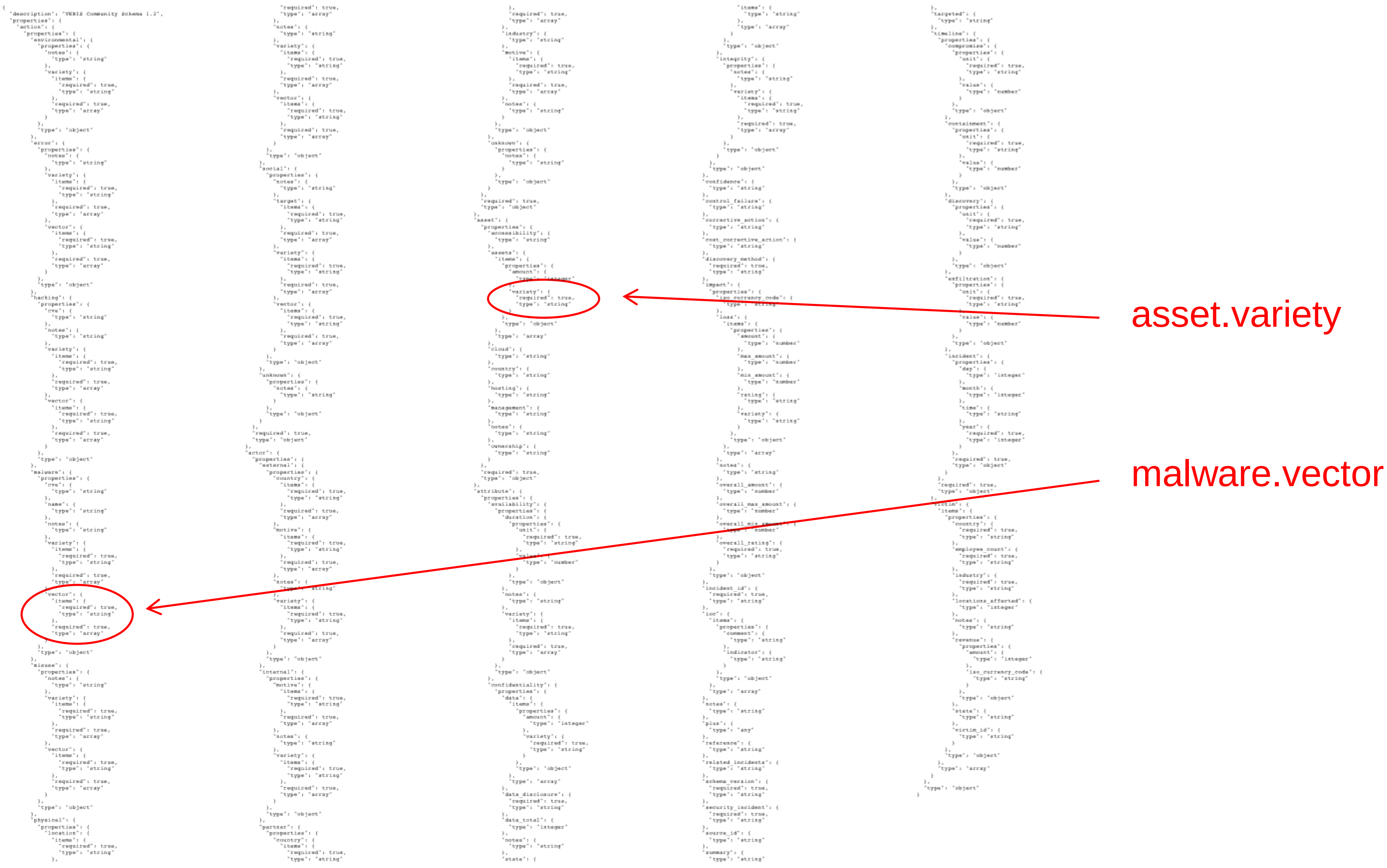
2014: specific patterns for specific recommendations

Last year, we noticed most breaches fit into patterns



111	POS smash-and-grab
190	Physical ATM
+ 120	Assured Penetration Technique
421	
÷ 621	Total Breaches
68%	

We can use the structured VERIS coding of an incident for statistical clustering



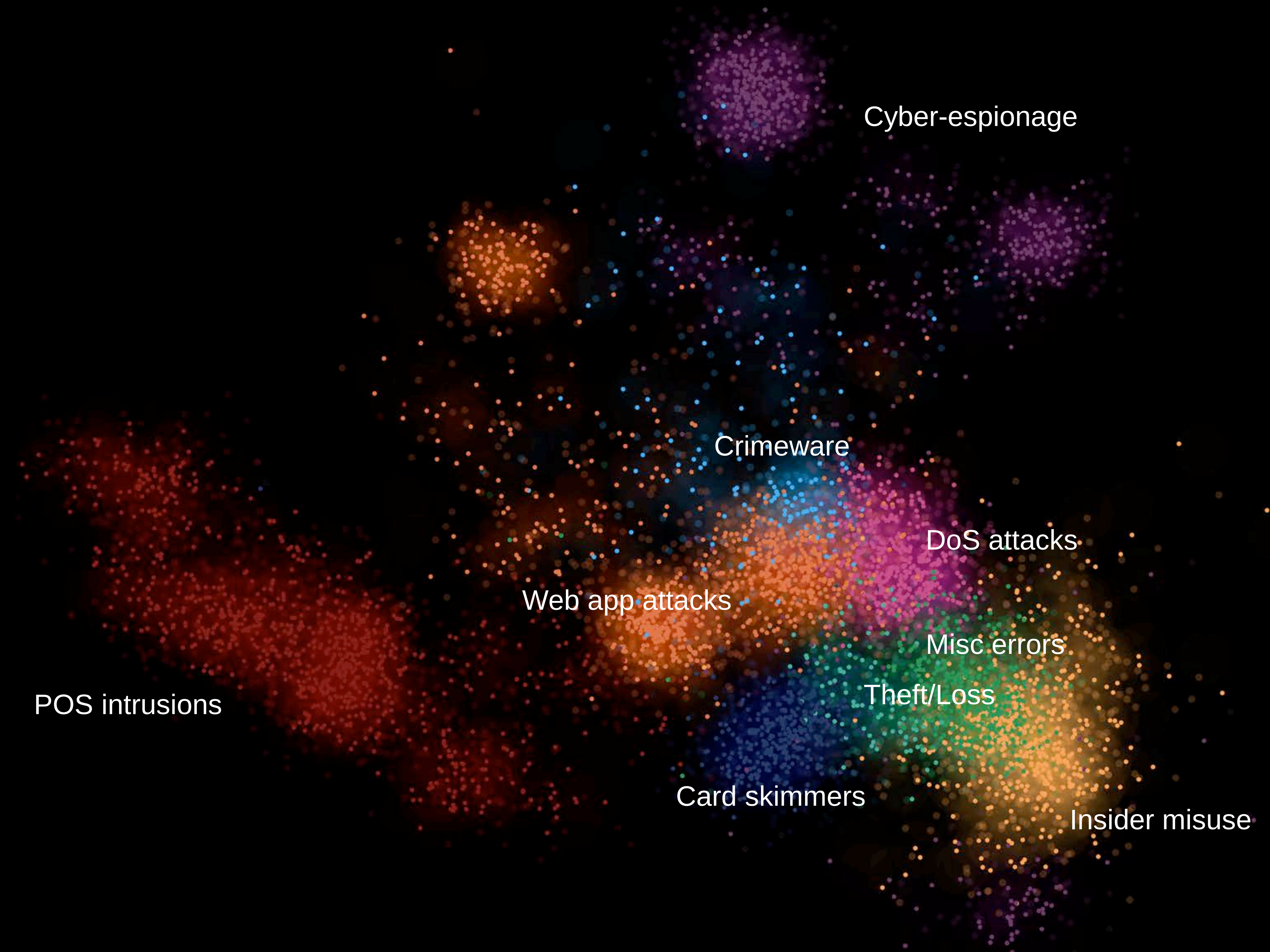
```
{
  "description": "VERIS Community Schema 1.2",
  "properties": {
    "action": {
      "properties": {
        "environmental": {
          "properties": {
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "error": {
          "properties": {
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "hacking": {
          "properties": {
            "cve": {
              "type": "string"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "malware": {
          "properties": {
            "cve": {
              "type": "string"
            },
            "name": {
              "type": "string"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "misuse": {
          "properties": {
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "physical": {
          "properties": {
            "location": {
              "items": {
                "required": true,
                "type": "string"
              },
```

```
              "required": true,
              "type": "array"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "social": {
          "properties": {
            "notes": {
              "type": "string"
            },
            "target": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "vector": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "unknown": {
          "properties": {
            "notes": {
              "type": "string"
            }
          },
          "type": "object"
        }
      },
      "required": true,
      "type": "object"
    },
    "actor": {
      "properties": {
        "external": {
          "properties": {
            "country": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "motive": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "internal": {
          "properties": {
            "motive": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "partner": {
          "properties": {
            "country": {
              "items": {
                "required": true,
                "type": "string"
```

```
              },
              "required": true,
              "type": "array"
            },
            "industry": {
              "type": "string"
            },
            "motive": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            },
            "notes": {
              "type": "string"
            }
          },
          "type": "object"
        },
        "unknown": {
          "properties": {
            "notes": {
              "type": "string"
            }
          },
          "type": "object"
        }
      },
      "required": true,
      "type": "object"
    },
    "asset": {
      "properties": {
        "accessibility": {
          "type": "string"
        },
        "assets": {
          "items": {
            "properties": {
              "amount": {
                "type": "integer"
              },
              "variety": {
                "required": true,
                "type": "string"
              }
            },
            "type": "object"
          },
          "type": "array"
        },
        "cloud": {
          "type": "string"
        },
        "country": {
          "type": "string"
        },
        "hosting": {
          "type": "string"
        },
        "management": {
          "type": "string"
        },
        "notes": {
          "type": "string"
        },
        "ownership": {
          "type": "string"
        }
      },
      "required": true,
      "type": "object"
    },
    "attribute": {
      "properties": {
        "availability": {
          "properties": {
            "duration": {
              "properties": {
                "unit": {
                  "required": true,
                  "type": "string"
                },
                "value": {
                  "type": "number"
                }
              },
              "type": "object"
            },
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        },
        "confidentiality": {
          "properties": {
            "data": {
              "items": {
                "properties": {
                  "amount": {
                    "type": "integer"
                  },
                  "variety": {
                    "required": true,
                    "type": "string"
                  }
                },
                "type": "object"
              },
              "type": "array"
            },
            "data_disclosure": {
              "required": true,
              "type": "string"
            },
            "data_total": {
              "type": "integer"
            },
            "notes": {
              "type": "string"
            },
            "state": {
```

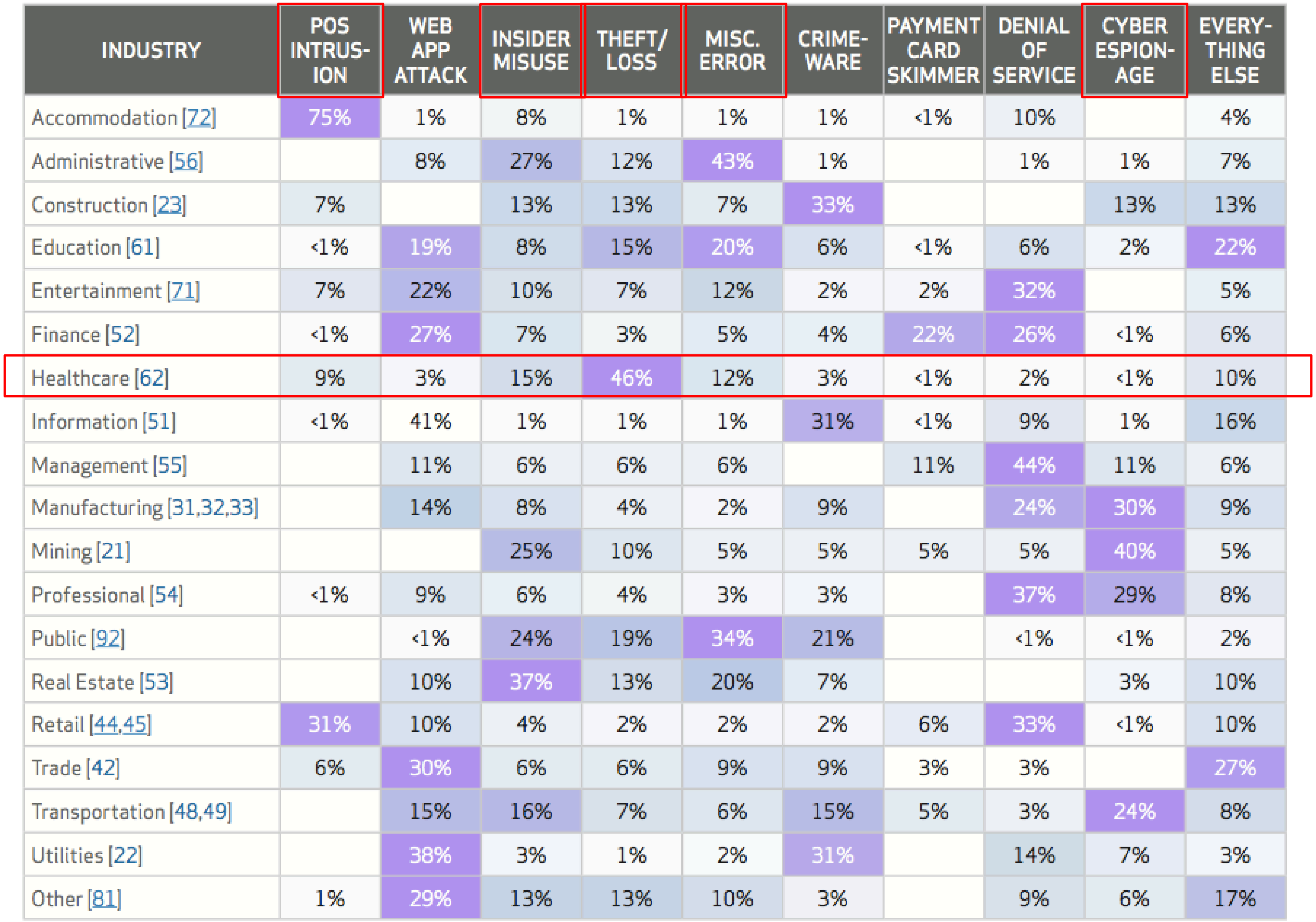
```
              "items": {
                "type": "string"
              },
              "type": "array"
            }
          },
          "type": "object"
        },
        "integrity": {
          "properties": {
            "notes": {
              "type": "string"
            },
            "variety": {
              "items": {
                "required": true,
                "type": "string"
              },
              "required": true,
              "type": "array"
            }
          },
          "type": "object"
        }
      },
      "type": "object"
    },
    "confidence": {
      "type": "string"
    },
    "control_failure": {
      "type": "string"
    },
    "corrective_action": {
      "type": "string"
    },
    "cost_corrective_action": {
      "type": "string"
    },
    "discovery_method": {
      "required": true,
      "type": "string"
    },
    "impact": {
      "properties": {
        "iso_currency_code": {
          "type": "string"
        },
        "loss": {
          "items": {
            "properties": {
              "amount": {
                "type": "number"
              },
              "max_amount": {
                "type": "number"
              },
              "min_amount": {
                "type": "number"
              },
              "rating": {
                "type": "string"
              },
              "variety": {
                "type": "string"
              }
            },
            "type": "object"
          },
          "type": "array"
        },
        "notes": {
          "type": "string"
        },
        "overall_amount": {
          "type": "number"
        },
        "overall_max_amount": {
          "type": "number"
        },
        "overall_min_amount": {
          "type": "number"
        },
        "overall_rating": {
          "required": true,
          "type": "string"
        }
      },
      "type": "object"
    },
    "incident_id": {
      "required": true,
      "type": "string"
    },
    "ioc": {
      "items": {
        "properties": {
          "comment": {
            "type": "string"
          },
          "indicator": {
            "type": "string"
          }
        },
        "type": "object"
      },
      "type": "array"
    },
    "notes": {
      "type": "string"
    },
    "plus": {
      "type": "any"
    },
    "reference": {
      "type": "string"
    },
    "related_incidents": {
      "type": "string"
    },
    "schema_version": {
      "required": true,
      "type": "string"
    },
    "security_incident": {
      "required": true,
      "type": "string"
    },
    "source_id": {
      "type": "string"
    },
    "summary": {
      "type": "string"
```

```
    },
    "targeted": {
      "type": "string"
    },
    "timeline": {
      "properties": {
        "compromise": {
          "properties": {
            "unit": {
              "required": true,
              "type": "string"
            },
            "value": {
              "type": "number"
            }
          },
          "type": "object"
        },
        "containment": {
          "properties": {
            "unit": {
              "required": true,
              "type": "string"
            },
            "value": {
              "type": "number"
            }
          },
          "type": "object"
        },
        "discovery": {
          "properties": {
            "unit": {
              "required": true,
              "type": "string"
            },
            "value": {
              "type": "number"
            }
          },
          "type": "object"
        },
        "exfiltration": {
          "properties": {
            "unit": {
              "required": true,
              "type": "string"
            },
            "value": {
              "type": "number"
            }
          },
          "type": "object"
        },
        "incident": {
          "properties": {
            "day": {
              "type": "integer"
            },
            "month": {
              "type": "integer"
            },
            "time": {
              "type": "string"
            },
            "year": {
              "required": true,
              "type": "integer"
            }
          },
          "required": true,
          "type": "object"
        }
      },
      "required": true,
      "type": "object"
    },
    "victim": {
      "items": {
        "properties": {
          "country": {
            "required": true,
            "type": "string"
          },
          "employee_count": {
            "required": true,
            "type": "string"
          },
          "industry": {
            "required": true,
            "type": "string"
          },
          "locations_affected": {
            "type": "integer"
          },
          "notes": {
            "type": "string"
          },
          "revenue": {
            "properties": {
              "amount": {
                "type": "integer"
              },
              "iso_currency_code": {
                "type": "string"
              }
            },
            "type": "object"
          },
          "state": {
            "type": "string"
          },
          "victim_id": {
            "type": "string"
          }
        },
        "type": "object"
      },
      "type": "array"
    }
  },
  "type": "object"
}
```


Cyber-espionage
Crimeware
DoS attacks
Web app attacks
Misc errors
Theft/Loss
POS intrusions
Card skimmers
Insider misuse

The frequency of patterns in an industry supports specific recommendations

Figure 19.
Frequency of incident classification patterns per victim industry



INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIMEWARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

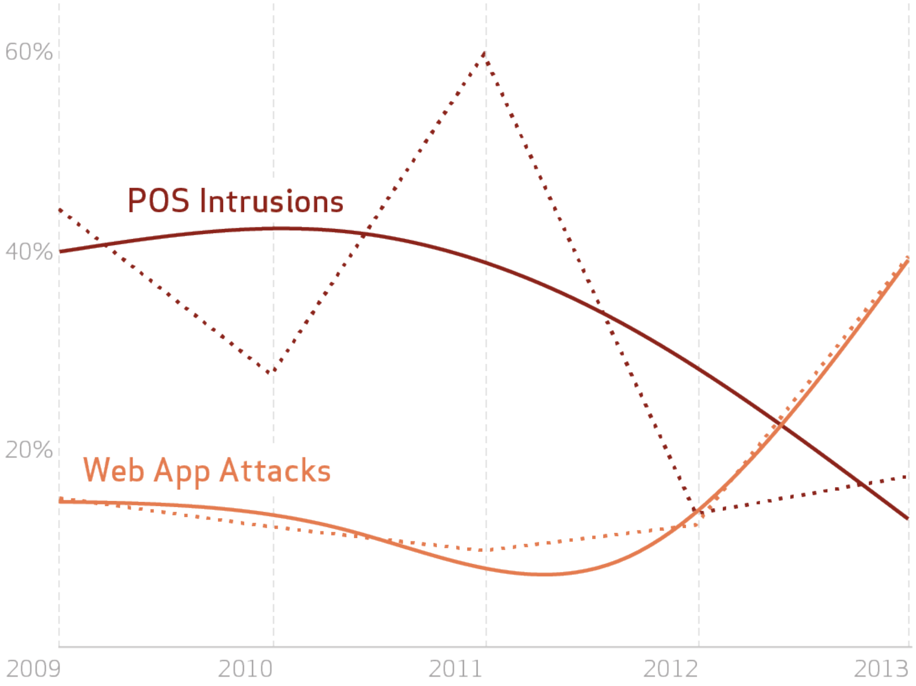
Point of Sale (POS) Intrusions

Remote attacks against the environments where retail transactions are conducted, specifically where card-present purchases are made.

Point of Sale Intrusion Key Findings

- Overall frequency is actually declining
- Brute forcing remote access to POS still primary intrusion vector
- Increased frequency of RAM scraping malware (versus key logging)
- Recommended controls:
  - Restrict remote access, mixed use
  - Enforce password policies
  - Deploy AV
  - Network segmentation
  - Network monitoring
  - 2-factor authentication

Figure 20.
Comparison of POS Intrusions and Web App Attacks incident classification patterns, 2011-2013



Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

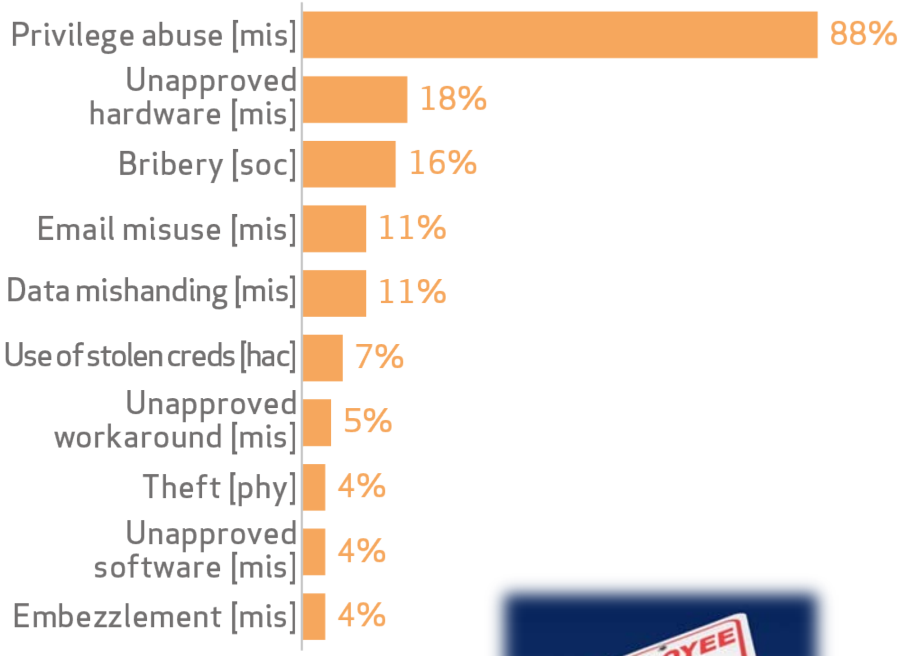
Insider and privilege misuse

Any unapproved or malicious use organizational resources.

Insider and Privilege Misuse Key Findings

- Most activity abuses trust necessary to perform normal duties
- Most incidents happen at the victim organization
- Motivation is primarily financial, with some espionage (to benefit a competitor)
- Internal detection is unusually common and fast
- Recommended controls:
  - Know your data and who has access to it
  - Review user accounts
  - Watch for data exfiltration
  - Publish audit results

Figure 30.
Top 10 threat action varieties within Insider Misuse (n=153)



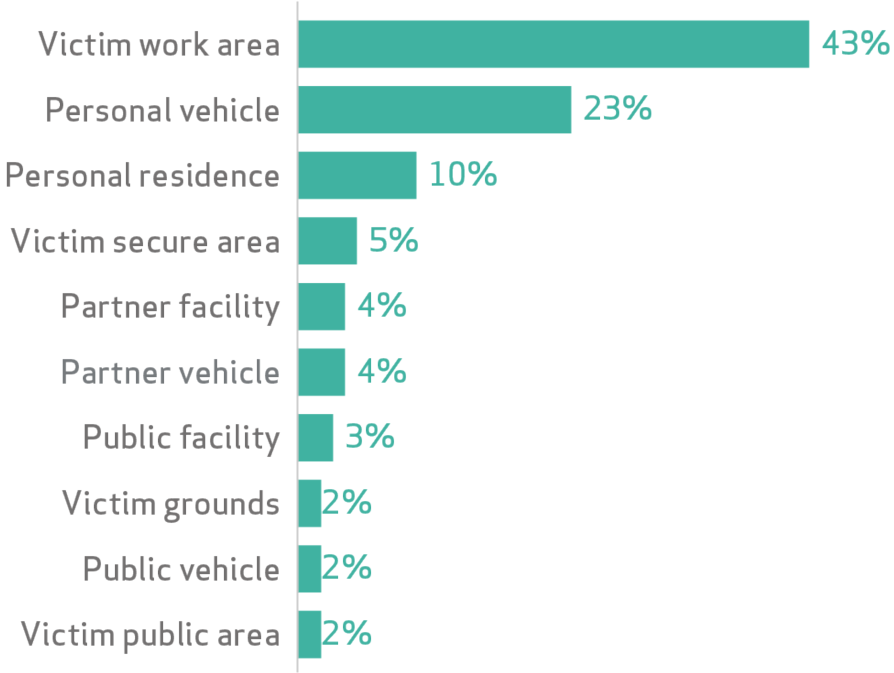
Physical Theft and Loss

Incidents where an information asset went missing, whether through misplacement or malice.

Physical Theft and Loss Key Findings

- Assets are stolen more often from offices than vehicles or residences
- Loss is reported more frequently than theft (15:1)
- More losses and thefts are reported because of disclosure regulations than fraud
- Data varieties at risk are mostly personal and medical
- Recommended controls:
  - Encrypt devices
  - Keep them with you
  - Back them up
  - Lock them down
  - Use unappealing tech

Figure 40.
Top 10 locations for theft within Theft/Loss (n=332)



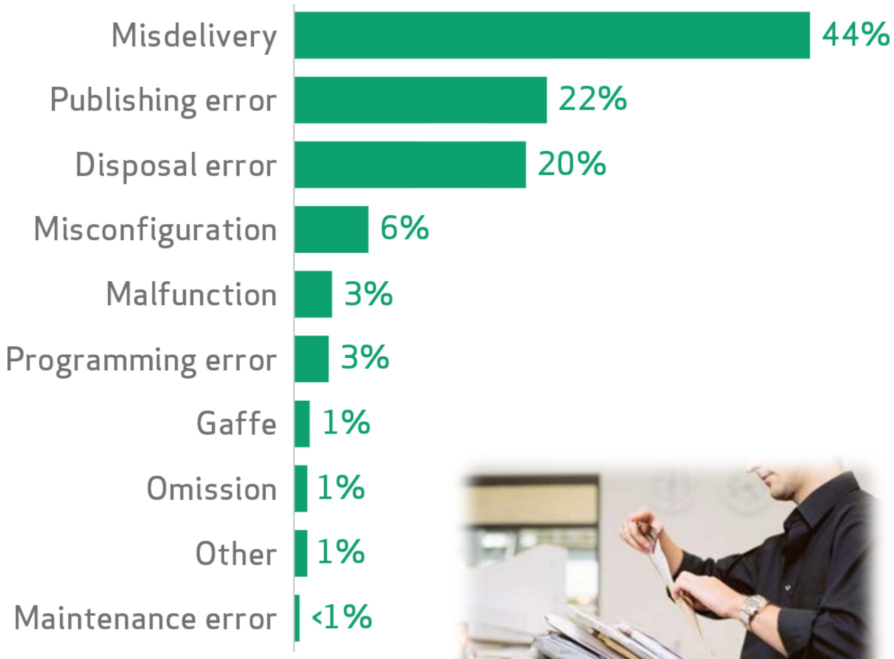
Miscellaneous errors

Incidents where unintentional actions directly compromised a security attribute of an information asset.

Miscellaneous Errors Key Findings

- Highly repetitive processes involving sensitive data are particularly error prone
- Discovery typically takes a long time, and it's external about two-thirds of the time
- Recommended controls:
  - Consider Data Loss Prevention (DLP) software
  - Tighten processes around posting documents
  - Spot-check large mailings
  - IT disposes of all information assets (and test them)

Figure 43.
Top 10 threat action varieties within Miscellaneous Errors (n=558)



Cyber espionage

Incidents in this pattern include unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage.

Cyber espionage key findings

- Most actors are state affiliated, but 11% are organized crime
- Cyber espionage involves many actions, but few initial vectors
- Discovery methods and times leave a lot of room for improvement
- Recommended controls:
  - Patching
  - Anti-virus
  - User training
  - Network segmentation
  - Good logging
  - Break the delivery-exploitation-installation chain
  - Spot C2 and data exfiltration
  - Stop lateral movement inside the network

Figure 58.
Variety of external actors within Cyber-espionage (n=437)

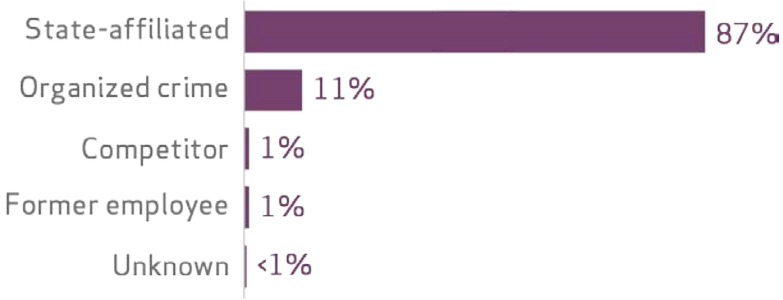
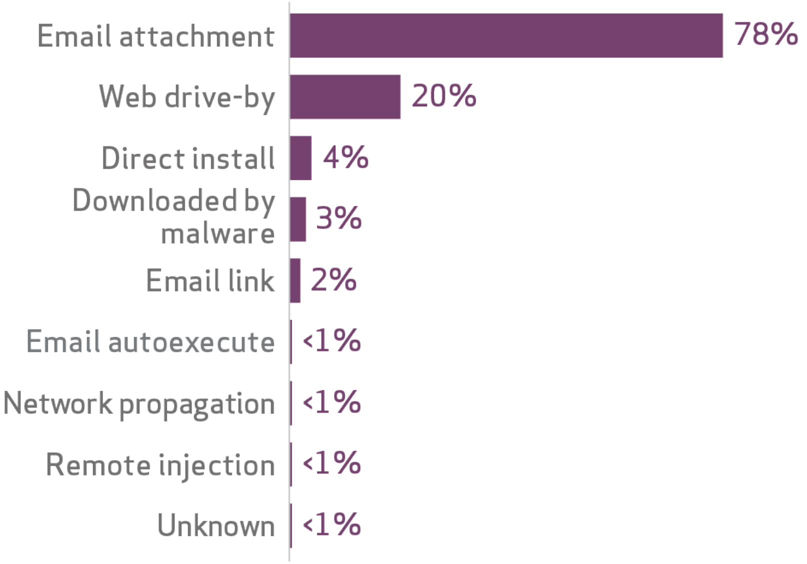
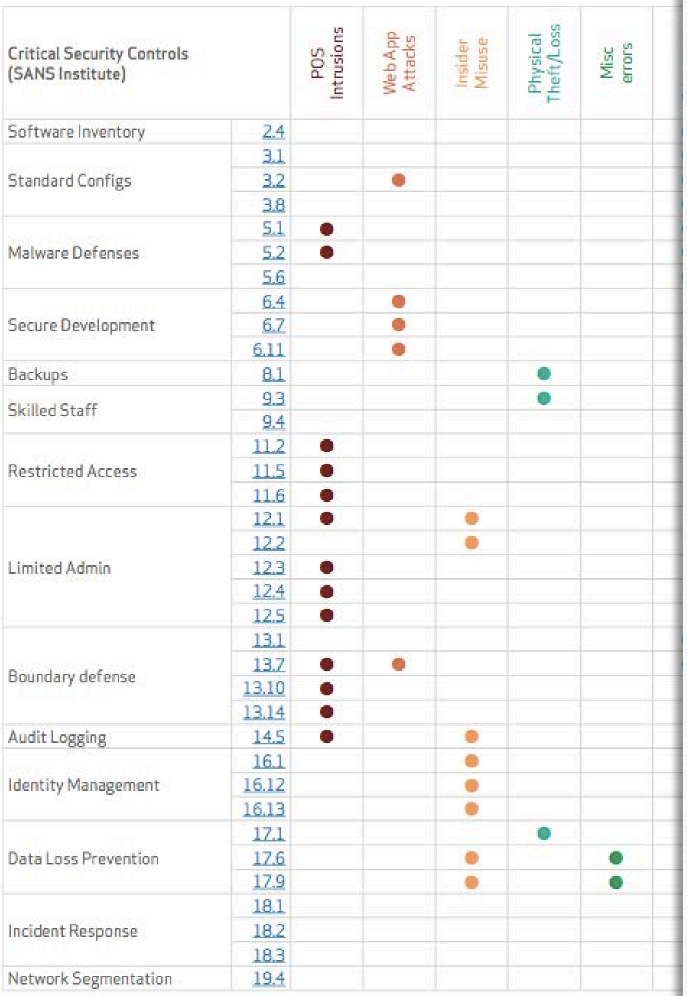


Figure 61.
Vector for malware actions within Cyber-espionage (n=329)



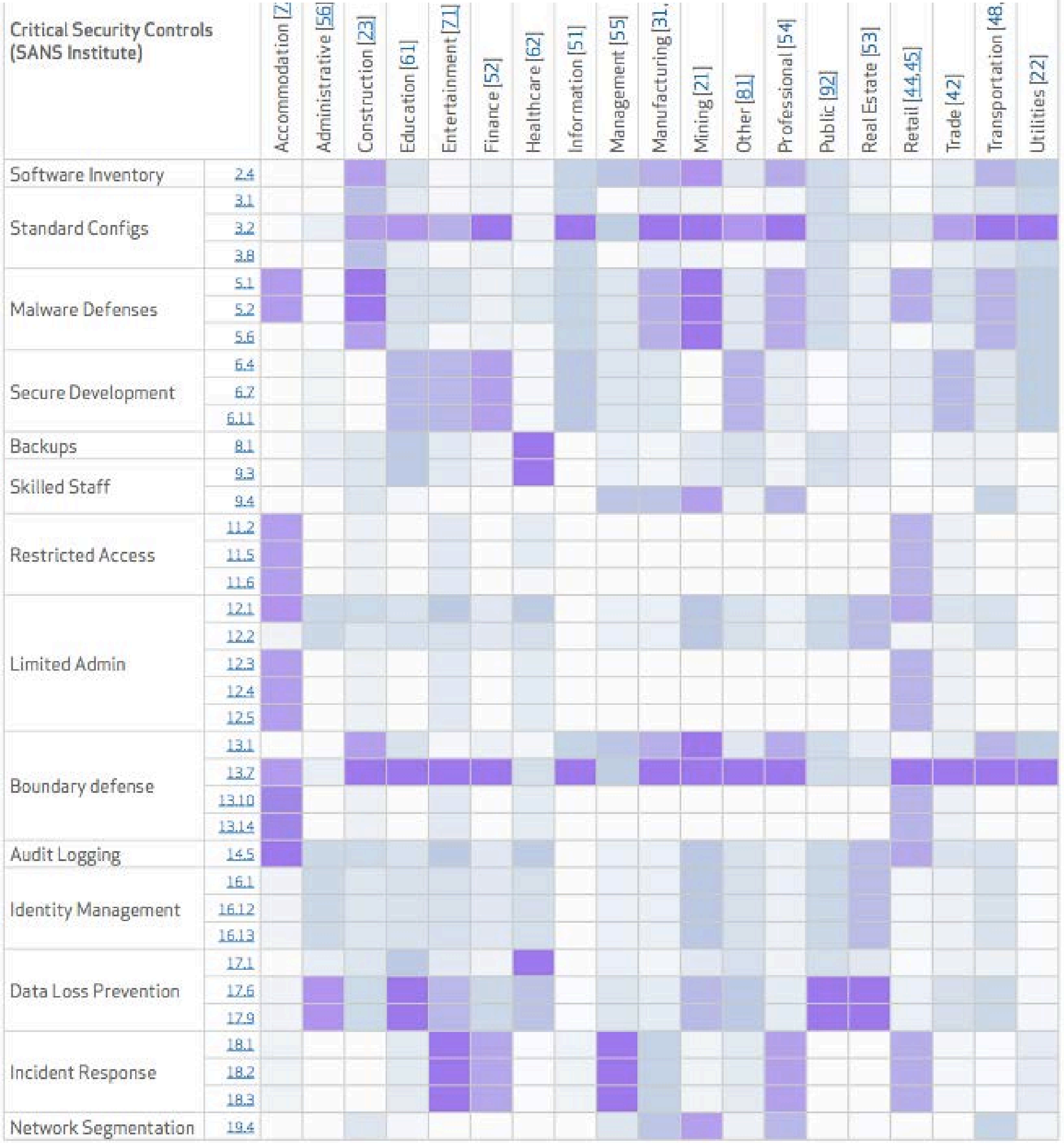
So what?

Figure 69.
Critical security controls mapped to incident patterns. Based on recommendations given in this



Critical Security Controls (SANS Institute)		POS Intrusions	Web App Attacks	Insider Misuse	Physical Theft/Loss	Misc errors
Software Inventory	2.4					
Standard Configs	3.1					
	3.2		●			
	3.8					
Malware Defenses	5.1	●				
	5.2	●				
	5.6					
Secure Development	6.4		●			
	6.7		●			
	6.11		●			
Backups	8.1				●	
Skilled Staff	9.3				●	
	9.4					
Restricted Access	11.2	●				
	11.5	●				
	11.6	●				
Limited Admin	12.1	●		●		
	12.2			●		
	12.3	●				
	12.4	●				
	12.5	●				
Boundary defense	13.1					
	13.7	●	●			
	13.10	●				
	13.14	●				
Audit Logging	14.5	●		●		
Identity Management	16.1			●		
	16.12			●		
	16.13			●		
Data Loss Prevention	17.1				●	
	17.6			●		●
	17.9			●		●
Incident Response	18.1					
	18.2					
	18.3					
Network Segmentation	19.4					

Figure 70.
Prioritization of critical security controls by industry. Based on frequency of incident patterns within each industry and recommendations for each pattern given in this report. The shading is relative to each industry.



Additional information is available

- Download: www.verizonenterprise.com/dbir
- VERIS: www.veriscommunity.net
- Email: DBIR@verizon.com
- Twitter: @vzdbir and hashtag #dbir
- Blog: http://www.verizonenterprise.com/security/blog/
- VERIS Community Database: http://vcdb.org