2014 Data Breach Investigations Report
TRANSPORTATION

This year’s Verizon Data Breach Investigations Report (DBIR) is based around nine incident classification patterns: common signatures that describe the vast majority of security incidents.

Just three of these nine patterns cover 55% of security incidents experienced by organizations in the transportation sector. Improving your defenses against these three areas could make your organization much more secure.

**CYBER-ESPIONAGE**

Espionage is not just a problem for government and military organizations. 24% of transportation incidents were cyber-espionage.

It’s easy to see why. Road, rail and air transport infrastructures are truly critical to nations’ operations, and one of the first targets for state-sponsored attackers looking to plan disruption.

It’s interesting that, while the array of tools used in cyber-espionage is diverse, the basic methods of gaining access to a victim’s environment are not.

78% of cyber-espionage attacks involved the use of a malicious email attachment. A well-crafted and personally relevant email is sent to targeted users, prompting them to open an attachment or click a link within the message. Inevitably, they take the bait, at which point malware installs on the system, a backdoor or command channel opens, and the attacker is in.

Last year 95% of attacks involved spear-phishing as described above. The drop reflects the rise in strategic web compromises (SWCs). Instead of email bait, SWCs set a trap within (mostly) legitimate websites that are likely to be visited by the target demographic. When a user visits the page, the trap is sprung, the system infected, and the attacker gains entry.

**What you can do:**

• **Patch promptly.** Exploiting software vulnerabilities is a common first step.

• **Use anti-virus, and keep it up to date.** It won’t protect you from zero-day attacks, but many still fall prey to well-known dangers.

• **Train users.** Give them the knowledge they need to recognize and report danger signs.

• **Keep good logs.** Log system, network, and application activity. This is a good foundation for incident response, and will support many proactive countermeasures.

---

*Data breaches can be extremely costly. The Verizon DBIR has, for years, been the best source of insight about the threat landscape. This year’s report covers over 63,000 security incidents from 95 countries.*

*This year’s DBIR uses statistical methods to identify ‘clusters’ of similar incidents and breaches. Just nine patterns cover 92% of the security incidents that we’ve analyzed over the last ten years.*

*Security incidents by pattern, transportation companies versus all industries, 2011–2013*
INSIDER MISUSE

Insider and privilege misuse accounted for 16% of incidents suffered by transportation organizations.

This category covers situations when employees, ex-employees, contractors and partners with access rights use their privileges to access data, either in person or over the network.

Culprits can come from every level of the organization, even senior executives.

In transportation, there's operational and sensitive commercial data to worry about, but also in many cases passenger payment details.

Most incidents of insider misuse were digital. Rather than sneaking paper files out in a bag, insiders used the corporate network 85% of the time. With the right credentials, it's easy to copy files to a USB drive without anyone noticing.

What you can do:
- **Know your data.** The first step in protecting your data is knowing where it is and who has access to it.
- **Review user accounts.** Having identified who has access to sensitive data, implement a process to continuously monitor user and system behavior as well as revoking access when employees change role or leave.
- **Watch the exits.** Set up controls to watch for data transfers out of the organization.
- **Publish anonymized results of audits.** Enforcing policies as part of a continuous monitoring program can be a powerful deterrent.

WEB APP ATTACKS

15% of incidents affecting transportation organizations were web application attacks. This pattern covers any incident in which attackers use stolen credentials or exploit vulnerabilities in web applications.

The transportation sector is increasingly adopting web technologies — for online journey booking and tracking in customer-facing services, and for collaboration and supply chain applications internally and with partners.

Technically, web app attacks are difficult to defend against. Attackers have a huge variety and combination of techniques available to breach your systems.

In our 2014 dataset, just under two out of every three web app attacks were attributable to activist groups driven by ideology. Public transport, air travel and freight are critical infrastructures in global society and commerce, so they make a prime target for those bent on causing disruption.

What you can do:
- **Use two-factor authentication.** Look at soft tokens and biometrics.
- **Consider switching to a static CMS.** Instead of executing code to generate the content for every request, pre-generate pages to reduce the opportunity for exploits.
- **Enforce lockout policies.** Locking accounts after repeated failed login attempts will help to thwart brute-force attacks.

Download the full report, infographic, and other DBIR resources from verizonenterprise.com/DBIR/2014

verizonenterprise.com