The security-minded Byrnes would doubtless be a shoo-in as CIO for any major corporation. Ninety-nine employees out of a hundred move from one organisation to the next with no intention of breaking the ‘circle of trust’. Every so often, however, former members of staff may try to take confidential information with them to their new employers or deliberately tamper with data on the system out of spite. Fortunately there are a number of things organisations can do to protect their data from such risks.

### References


### Mounting evidence

Verizon’s ‘2017 Data Breach Investigations Report’ (DBIR) highlights how privilege abuse by insiders continues to be a common source of attacks. Threats that come from within are particularly difficult to detect, often taking months, or even years, to discover.
Elsewhere, in a 2017 study involving more than 700 IT professionals, 66% of respondents rated company insiders as the primary threat to security and systems availability.2 Drilling down further into insider threat data, a 2016 report found the biggest threat to be privileged users, such as managers with access to sensitive information (60%).3 Other key risks were said to be contractors and consultants (57%), followed by regular employees (51%).

“Data volumes are growing ever larger. As a consequence there are plenty of opportunities for employees to abuse their network privileges before they leave”

Virtual and hybrid cloud technologies are making IT infrastructures more complex. At the same time, data volumes are growing ever larger. As a consequence there are plenty of opportunities for employees to abuse their network privileges before they leave. According to the 2017 Verizon DBIR, this commonly manifests itself in the form of sensitive data being stolen, disclosed or in extreme cases destroyed. Stolen data is most often comprised of sales projections, marketing plans, sales leads and other types of intellectual property. In 15% of cases, an employee steals data to help him start up a competing company or to take to a new employer.

Real-world instances

The way researchers and industry experts constantly refer to the insider threat carries the risk that customers may simply ignore the warnings. However, there are plenty of real-world examples to point to. The threat to data from employees whose time with the organisation is ending is greatest if their employer is associated with healthcare, finance or retail. Over the past few years, each sector has seen a number of notable cases.

Healthcare: There are plenty of incidents where health workers have either misused patient data or attempted to steal confidential information. A recent example is the Med Centre Health breach in the US where an agency employee allegedly stole protected health information pertaining to 160,000 patients and provided it to unauthorised third parties in exchange for remuneration.4 In another occurrence, a disgruntled former employee stole the records of 15,000 patients at a plastic surgery clinic in Rodeo Drive, California.5 Meanwhile, in the UK, a BUPA employee inappropriately copied and removed information relating to 547,000 international health insurance plan customers.6

Finance and banking: You don’t have to look far to find examples here either. In 2016, the Office of the Comptroller of the Currency in the US disclosed a data breach involving an ex-employee’s unauthorised removal of more than 10,000 records which he had downloaded onto two thumb drives before retiring from the agency.7 A more recent example is the case of former JPMorgan

The types of insider threats that organisations are most concerned about. Source: ‘Insider Threat Spotlight Report’.
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات