KEYFACTOR

The ROI of PKI: Highlights from the Keyfactor-Ponemon Institute 2019 Report
The Impact of Unsecured Digital Identities

Working with Ponemon Institute, a leading cybersecurity research firm, Keyfactor set out to understand the challenges organizations face with PKI deployment, and quantify the real costs to businesses in managing — or mismanaging — digital identities and cryptographic keys.

The report highlights concerns from every industry that insufficient and ineffective digital identity management is putting organizations at significant risk.

Overview

As the demand for digital security grows and budgets begin to align, many companies have overlooked the critical importance of effective management of digital identities. As the first study of its kind, the Keyfactor-Ponemon Institute 2019 Report *The Impact of Unsecured Digital Identities* quantifies the breadth, scope and impact of what happens when PKI policies and processes are not at their best.

Think of your organization as an entity with identities. These identities are made up of people, applications and devices. To create a secure environment, **every identity** within the organization must be covered by layers of digital security.

Working with Ponemon Institute, a leading cybersecurity research firm, Keyfactor set out to understand the challenges organizations face with PKI deployment, and quantify the real costs to businesses in managing — or mismanaging — digital identities and cryptographic keys. Gathering input from nearly 600 respondents, the report highlights concerns from every industry that insufficient and ineffective digital identity management is putting organizations at significant risk.

What the report uncovered is that lack of visibility, certificate mismanagement, and reduced budgets leave businesses open to both security and financial risks. Lack of qualified staff and/or expertise, deficient process management, along with compliance failures, all pave the way for ineffective digital security that may be impacting your organization's bottom line.

Key Findings

Ponemon Institute developed five industry scenarios that addressed real and potential risks around ineffective key or certificate management. The data confirms what Keyfactor has learned from over fifteen years of engagements with global brands:

- Mismanagement of keys and certificates are of great concern to those who are responsible for them.

- Most organizations lack visibility into how many keys and certificates are deployed and when they expire.

- Outages impact both productivity and customer satisfaction.

- Compliance is impacted by insufficient practices and policies.

- Quantum computing needs to be addressed sooner rather than later.

KEYFACTOR

THE ROI OF PKI

PKI plays a critical role in the holistic strategy of securing your enterprise. As such, ineffective key and certificate management results in issues that not only affect IT, but impact the organization as a whole.

OUTAGES

74%

of respondents agree that digital certificates have caused un-planned downtime and outages. Outages due to certificate expira-tions cost organizations more than **$11.1M**.

FAILED AUDITS OR COMPLIANCE

77%

of respondents indicated that a failed audit or lack of compliance due to insufficient key manage-ment practices is a serious issue.

SECURITY STRIKES

$13.2M

The cost of a CA compromise, a "man in the middle" or phishing attack, is almost **$3.5M** in dimin-ished brand reputation alone, with a total cost of **$13.2M** to the organization.

Outages

Seventy-four percent of respondents agree that digital certificates have caused unplanned downtime and outages. **Over one-quarter** of respondents said that an unplanned outage due to certificate expiration has happened more than **four times in the past 24 months**. This downtime isn't just a nuisance. Between revenue loss, time required of administrative and customer support staff, lost productivity, and diminished reputation, outages due to certificate expirations cost organizations more than **$11.1M.**

Failed Audits or Compliance

Respondents were asked to rate the seriousness of a failed audit or lack of compliance due to insufficient key management practices. **Seventy-seven percent** indicated that this is a serious issue. Determining how many keys are in use and concerns about being able to secure keys throughout their lifecycle – from generation through revocation – is also troubling. **Less than half** believe they are able to hire and retain qualified IT security personnel and only **36%** of IT security staff are dedicated to PKI deployment. Inadequate processes and insufficient staffing landed compliance misses at a **$14.4M** price tag per-organization.

Security Strikes

Certificate Authorities (CAs) play a core role in effective PKI management. Bad actors attempt to infiltrate organizations through any gap they can find and compromising a CA and issuing unauthorized certificates is a real threat. The report data found that there is a **38%** likelihood that organizations will experience a CA compromise, a "man in the middle" or phishing attack over the next two years. The cost of this kind of occurrence is almost **$3.5M** in diminished brand or reputation alone, with a total cost of **$13.2M** to the organization.

It's clear from the responses that PKI is generally an under-budgeted and under-resourced area within IT security. It's also a budget line item without clear ownership and as such, it's hard to drive accountability.

These are a small sample of the report's findings, and we expect they will spark a discussion about your organization's management of digital identities. To dive deeper into the data, get your copy of the report here. For more information or to contact one of our experts, visit www.keyfactor.com.