2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

GLOBAL EDITION

EXECUTIVE SUMMARY

One of the fundamental challenges of cybersecurity is dealing with the speed of change. With each new computing paradigm shift – Cloud, Big Data, IoT etc. – come new capabilities and possibilities – along with new security vulnerabilities to be exploited. It's no wonder that the security industry overall now tallies in excess of 1,400 vendors by 451 Research's count, with as many as nine new startups per month and roughly 10 new security categories created each year.

#2017DataThreat

EXECUTIVE SUMMARY

Glass half-full, or half-empty?

Similar to last year, the overall assessment of this year's Thales Data Threat Report depends on one's perspective. Security vendors, practitioners and even attackers are likely to find a mixture of both encouraging trends, but also warning signs – all set against a backdrop of attacks that seem to grow more successful each year.

On the positive side, one potentially encouraging sign – at least for security vendors – is that 73% of respondents anticipate security spending increases in the next 12 months, a sharp increase from 58% last year. The primary reason for the jump is that those who anticipate 'much higher' spending (23%) nearly doubled from just 12% last year, also potentially good news for practitioners dealing with security budget constraints. Furthermore, while most security spending remains driven by compliance concerns, security spending in order to implement best practices has moved up again for the second straight year and into the #2 overall spot, a sign that enterprises are starting to do more than the bare minimum to meet regulatory demands. We should also note that 2016 is also shaping up to be a banner year for investment bankers.

However, despite the higher spending (and planned spending) on security, some 26% of respondents said their organizations experienced a breach in the last year, up from 21.7% in 2016, while 42% of respondents experienced a data breach at another time in the past (up from 39.3%). It is no wonder then that nearly one in three respondents feel their organizations are either 'very vulnerable' or 'extremely vulnerable' to threats to sensitive data. Overall, the research suggests that the security industry looks increasingly like a dog chasing its own tail – despite more and more money spent on security each year, our collective problems continue to worsen.

One possible explanation for this vicious cycle is that organizations keep spending on the same solutions that have worked in the past but are no longer the most effective at stopping modern breaches. For example, similar to last year's study, network and endpoint security topped the list of planned spending categories, yet endpoint security ranked at the bottom of the list in terms of effectiveness at preventing data breaches and data theft.

As an example, this year's research surveyed about container usage. Containers, at a high level provide another layer of abstraction that enable flexibility and portability regarding where applications can run, whether on premises, public cloud or private cloud. Just over two years old, Docker – an open source container iteration – is proliferating rapidly in various organizations seeking to speed up application development. One of the more noteworthy data points from this year's study is that nearly 40% of respondents are already using containers in production environments, yet like other emerging technologies, 47% of respondents view security as the main adoption barrier for containers, the number one response other than budget (44%).

"73% OF RESPONDENTS ANTICIPATE SECURITY SPENDING INCREASES IN THE NEXT 12 MONTHS, A SHARP INCREASE FROM 58% LAST YEAR."

KEY FINDINGS:

- More than two in three respondents (67.8%) said their organizations have been breached at some point, an increase of nearly 7% percent over the previous year. And more than one in four (26%) were breached in the last year alone, up from 21.7% the previous year.

- The overwhelming majority of respondents still feel some degree of vulnerability to data threats (88%), down slightly from the previous year (90%), but still at an alarmingly high level. Those feeling 'extremely vulnerable' rose slightly, to 9.1% from 8.2%.

- Compliance (44%) remains the primary reason for spending on data security by a stubbornly wide margin over implementing security best practices, the second strongest driver (38%). However, we found it encouraging that fewer respondents (59.5%) viewed compliance requirements as 'very or extremely effective', a notable drop from 64% last year. Meanwhile brand and reputation plummeted to 36%, down markedly from 50% in last year's study as a primary reason for security spending.

- In a departure from both practical experience and anecdotal evidence, more than 57% of respondents claim 'complete knowledge' of where sensitive data is located, up sharply from 42% last year.

- Data sovereignty has become a hot topic in light of concerns about new regulations, and government snooping. Encryption was identified as the clear choice (64%) to satisfy local data privacy laws such as the EU's recently approved General Data Protection Regulation (GDPR). Tokenization (40%) is listed as a distant second, while migrating data to jurisdictions or choosing local cloud providers are at the very bottom of the list.

- Complexity remains the top barrier to more aggressive adoption of data security solutions chosen by 50.4% of respondents. 'Lack of staff' trailed by a considerable margin in second place at 36%.

- Though still a nascent technology that's been in the market for barely two years, Docker containers are being used by four in ten respondents for production applications, with a nearly 50-50 split between critical and non-critical applications. Only 13% of respondents have no plans to use Docker containers in the year ahead. Like other emerging technologies like cloud, Big Data and (IoT), not surprisingly, security remains the #1 Docker adoption barrier (46.7% of respondents) and the #1 method for securing containers is encryption.

RE-PRIORITIZE YOUR IT SECURITY TOOL SET	With increasingly porous networks, and expanding use of external resources (SaaS, PaaS and IaaS most especially) traditional end point and network security are no longer sufficient. Look for data security tool sets that offer services-based deployments, platforms and automation that reduce usage and deployment complexity for an additional layer of protection for data.
DISCOVER AND CLASSIFY	Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT.
DON'T JUST CHECK OFF THE COMPLIANCE BOX	Global and industry regulations can be demanding, but firms should consider moving beyond compliance to greater use of encryption and BYOK, especially for cloud and other advanced technology environments.
ENCRYPTION AND ACCESS CONTROL	Encryption needs to move beyond laptops and desktops. **Data center:** FDE offers very limited protection in the data center – consider file and application level encryption and access controls. **Cloud:** Encrypt and manage keys locally, BYOK is an enabler for enterprise SaaS, PaaS and IaaS use. **Big Data:** Employ discovery as a complement to encryption and access control within the environment. **Containers:** Encrypt and control access to data both within containers and underlying data storage locations. **IoT:** Use secure device ID and authentication, as well as encryption of data at rest on devices, back end systems and in transit to limit data threats.

THALES

www.thales-esecurity.com