The Secure Cloud:

451 Research looks into the cloud to see what's driving the purchase of cloud security technologies.

Working from survey data and extensive interviews of information security executives by 451 Research service TheInfoPro (TIP), a new report analyzes some of the most interesting trends to complement vendor analysis by the 451 Enterprise Security Practice team. In a January 2014 report, 451 Research looked into what security products are underutilized or not utilized at all within enterprises. The research highlighted several key themes consistent across buyers and vendors regarding security purchases that did not deliver on their initial promise, but it didn't detail why the security technologies were purchased in the first place – other than a subset claiming a particular technology was purchased to satisfy a specific compliance need.

Compliance aside, a company saying it bought a product for 'security' doesn't offer much insight. What aspect of security is a product purchased for? What is the risk posture of the organization? And how is the security executive looking to maintain that risk posture among the disruptive roar of cloud and bring-your-own-device (BYOD) technologies?

Key Findings

+ Information security budgets continue a successful multi-year run of increases, mostly in the 5-10% range year over year.
+ Mobile device management (MDM) is a top project as well as a top source of pain among security managers.
+ Compliance continues to take a lion's share of security budget in the greatest percentage (47%) of enterprises, with data-loss prevention (DLP), security information and event management (SIEM) leading the charge. The majority of security executives we spoke with (49%) report into the CIO, which may be a contributing factor toward the compliance drive.
+ The greatest percentage of enterprises (57%) are making do with between 1 and 10 dedicated information security professionals.
+ Despite user behavior's perennial appearance as a top pain point, a plurality of enterprises (35%) only spend between 1 and 50 hours on security awareness training per year. User behavior is hard to measure and difficult to affect with technology alone, which likely contributes to apathy.
+ Despite the hype, threat intelligence continues to grow at a modest rate and investment in public cloud security remains low.
+ Outside of hard drives, laptops and email, encryption has not penetrated deep into the enterprise to help address data-level protection.
+ A side effect of cloud and BYOD is that a lot of 'old' technologies are having somewhat of a renaissance, with DLP and network access control (NAC) leading the way followed by encryption and identity and access management (IAM).

Macro Trends: Budgets, Compliance, and Aches and Pains

Many businesses are undergoing a digital transformation with more and more functionality being placed in technology systems. This, coupled with the rise of a greater variety of external threats, means spending has not slowed for security. Due to the very public nature of some breaches, many CISOs are subject to 'newspaper projects' – i.e., security initiatives resulting from the CEO reading about a competitor breach in the newspaper.

Putting external threats aside, the rapid pace of change being set by many organizations is causing challenges for security departments embedded in traditional business processes. These changes are fundamentally shifting not just how security is implemented, but how the business operates as a whole.

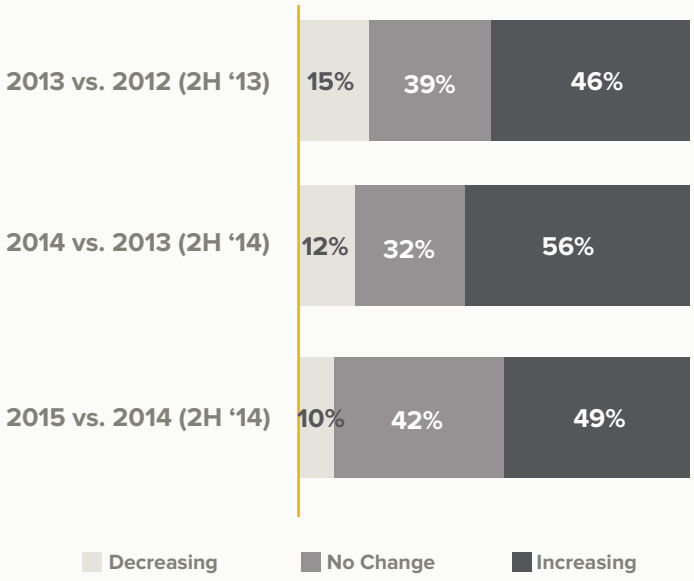
Even as traditional drivers such as compliance keep security spending buoyant, the nature in which it is applied to new environments such as cloud has brought about a change in spending.

Budget Trends

Information security budgets are continuing a successful multi-year run of increases, mostly in the 5-10% range year over year. More than half (56%) of security managers participating in the Wave 17 study noted a budget increase in 2014, against only 12% noting a lesser budget than 2013 (see Figure 1). 2015 is similarly positive with 49% of managers projecting a future increase.

Info Security Spending Continues To Increase

Figure 1:



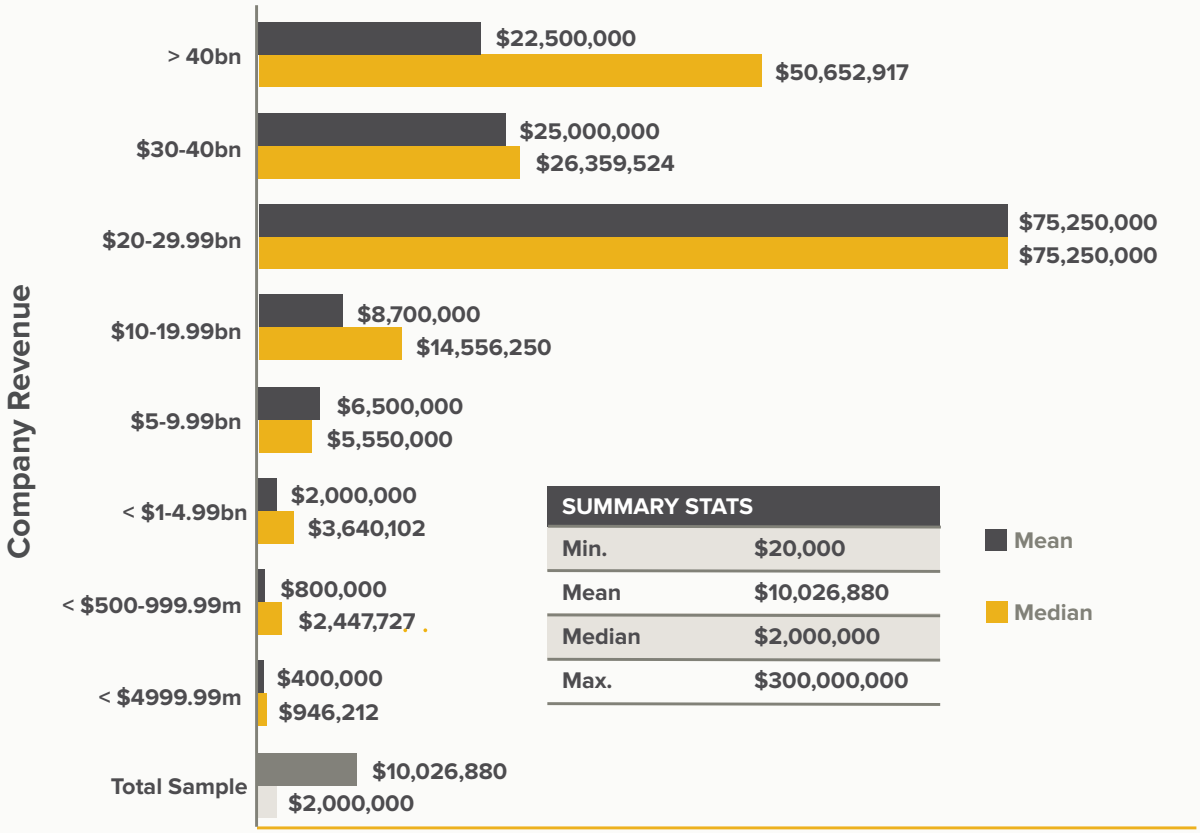
SOURCE: 451 RESEARCH'S THEINFOPRO INFORMATION SECURITY STUDY – WAVE 17

Looking at budget spend by revenue of the organization, enterprises with a turnover of $20bn-$29.99bn had the largest security budgets, on average spending just over $75m (see Figure 2). However, it is likely that a smaller sample fell into this category, resulting in the same median and mean figures.

Mean and Median 2014 Info Security Budgets, by Company Revenue

Figure 2:

What is your total Information Security budget in 2014, including both capex and opex? (US$)



SOURCE: 451 RESEARCH'S THEINFOPRO INFORMATION SECURITY STUDY – WAVE 17

:

Ouch, It Hurts

While the security industry has continued to grow, so has the volume and frequency of security breaches. This has caused many awkward boardroom discussions and even resulted in some c-level executives' heads rolling. If failures are imminent, then there doesn't appear to be much reason to continue the security spend.

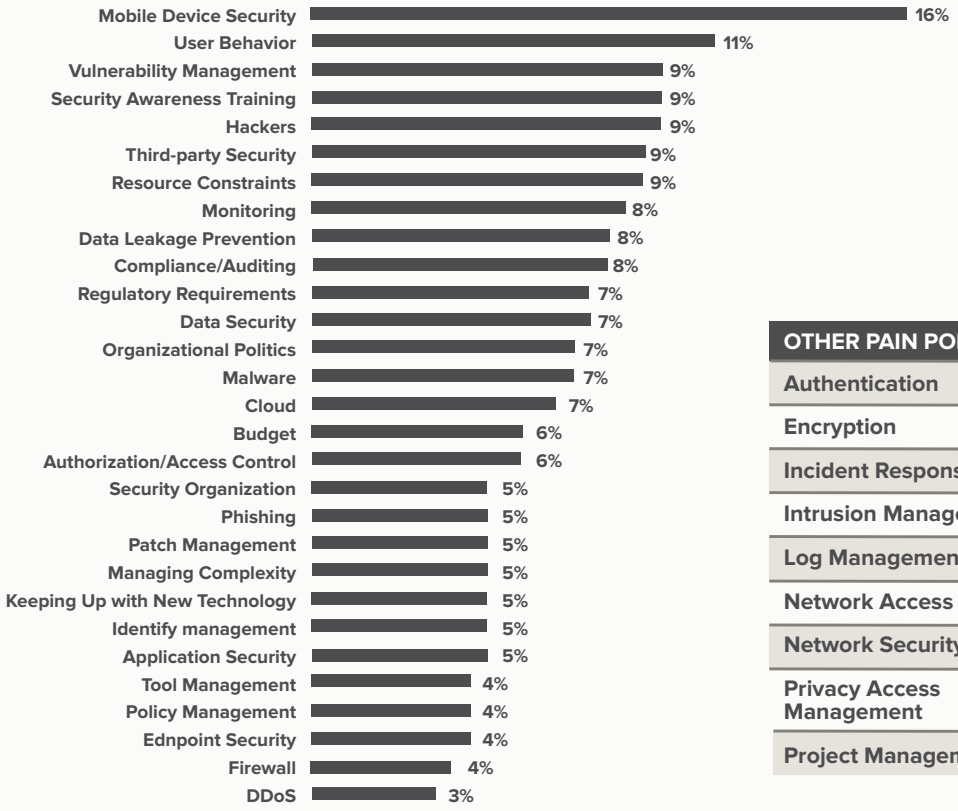
To understand security spending, one has to understand the motivation or pain behind the buying decision – that is, pain on the part of the security managers and the aspects of the job they find the most difficult.

As BYOD projects continue to proliferate through organizations, mobile device security emerged ahead of the pack and had 16% of security professionals reaching for the nearest painkillers (see Figure 3). It is interesting to note that the commentators focused on the problem of security rather than the solution of MDM.

Top Information Security Pain Points

Figure 3:

What are your top information security pain points? List up to three.



OTHER PAIN POINTS CITED	
Authentication	Remediation
Encryption	Remote Access
Incident Response	Risk Assessment
Intrusion Management	Security Operations
Log Management	SIEM
Network Access Control	Single Sign On
Network Security	Threat Intelligence
Privacy Access Management	Wireless Security
Project Management	

SOURCE: 451 RESEARCH'S THEINFOPRO INFORMATION SECURITY STUDY – WAVE 17

Among security professionals, the need, value and impact of user awareness, training and education are often debated. Often branded as the weakest link, users find themselves caught in the middle of security departments that view their behavior as risky and painful and, on the other side, increasingly targeted and sophisticated attacks such as spear phishing. Enterprise security teams have the not-so-envious task of educating their user bases about secure practices, such as not reusing passwords while at the same time teaching them how to remain vigilant against attacks and report suspected incidents. Despite user behavior being cited a top pain point, 35% of enterprises only spend between 1 and 50 hours on security awareness training per year. This is likely due to companies' inability to measure the effectiveness or return on investment of such activities. Some companies we've spoken to that have invested more time in training have reported that over time they have seen users shift from being a liability to an asset.

Although it's a mature technology, vulnerability management also remains high on the list of pains as security managers play the ongoing game of chasing after their own tails to deploy, patch, manage and change systems.

Hackers remained a consistent pain point alongside third-party security, which isn't surprising particularly in light of instances where attackers have breached a third party to gain access to critical internal resources, as in the case of Target, Sony and others.

Putting It All Together

A lot of enterprises continue spending on compliance initiatives as if it is an integral part of security. There may be several underlying factors that contribute to this, most notably the reporting line of the security executive. In most cases, reporting into the CIO could be seen as detrimental, and in some cases it may represent a conflict of interest where the CIO is a sponsor for an IT initiative.

Security is also an area where many organizations struggle to justify cost and return on investment. In such circumstances, compliance becomes a relatively quick win against which progress can be measured and benchmarked. However, all too often we have seen security become the casualty of departments that overzealously pursue compliance initiatives.

BYOD is a revolution that still appears to have many security managers on the back foot. An MDM offering may have seemed like the perfect panacea, but many have arrived at the conclusion that managing the device does not necessarily equate to protecting the data, and securing information in a legal manner represents its own set of challenges.

For all the talk that surrounds it, only 10% of enterprises have any tools to secure data in public cloud environments. Encryption, while slowly being adopted, is still very low compared to traditional hard drive, laptop and email encryption deployments. Similarly, while we've heard many a CISO grumble about the ineffectiveness of traditional antivirus offerings, none of them appear inclined to replace them in favor of next-gen endpoint protection technologies. We have seen some anecdotal evidence of some enterprises utilizing a next-gen endpoint product in conjunction with a lightweight or even free antivirus offering, but it will take a brave CISO to remove antivirus completely. Similarly, threat intelligence, despite its apparent hype in the market, has grown only modestly as companies look to find the best uses for it.

We've been hearing that the network perimeter is dead for many years now. If these rumors are to be believed, in the world of SaaS applications and BYOD, the network is about as useful as a chocolate teapot. CISOs may share that sentiment, but their wallets certainly don't, with spending on traditional and NGFWs showing no signs of slowing down.

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, 451 provides essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

Data Centers Powered by People

QTS Realty Trust, Inc. (NYSE: QTS) is a leading national provider of data center solutions and fully managed services and a leader in security and compliance. The company offers a complete, unique portfolio of core data center products, including custom data center (C1), colocation (C2) and cloud and managed services (C3), providing the flexibility, scale and security needed to support the rapidly evolving hybrid infrastructure demands of web and IT applications. With 12 data centers in eight states, QTS owns, operates and manages approximately 4.7 million square feet of secure, state-of-the-art data center infrastructure and supports more than 850 customers. QTS' Critical Facility Management (CFM) can provide increased efficiency and greater performance for third-party data center owners and operators.

For more information about QTS, please visit www.qtsdatacenters.com, call toll-free 877.QTS.DATA or follow us on Twitter @DataCenters_QTS.