Information Security Trends:

Preventing/Detecting Insider Espionage Not Adequately Covered

A June survey of 651 members of the 451 Global Digital Infrastructure Alliance focused on key information security trends, including overall spending and implementation status, as well as pain points and concerns.

90-Day Spending. A total of 52% of respondents say their organization's information security spending will increase over the next 90 days – up four points from the previous survey in February. Only 3% say spending will decrease.

Security Technology In Use/Pilot. *Firewall* (89%) and *Web Content Filtering* (80%) are the two most widely adopted security technologies in use. Just over three-quarters of the respondents use *Vulnerability Management* (76%) solutions.

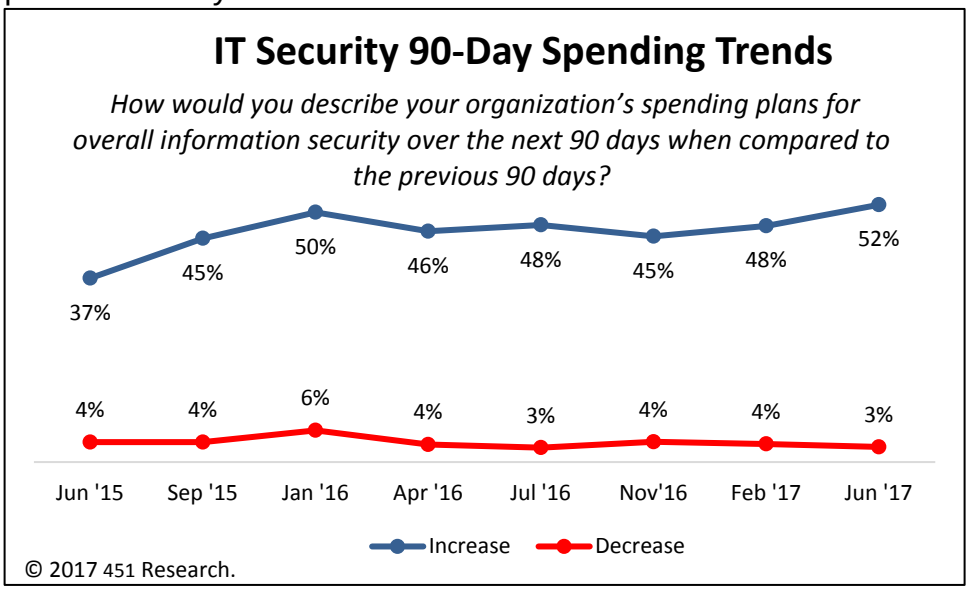
Top Pain Points. Respondents were asked to select the top security pain points, and *User Behavior* (30%) is the largest, followed by *Accurate, Timely Monitoring of Security Events* (22%) and *Staffing Information Security* (21%).

Inadequately Addressed Security Threats. Respondents were also asked which security threat they believe is currently inadequately addressed within their organization. The internal problem of *Preventing/Detecting Insider Espionage* (29%) tops the list.

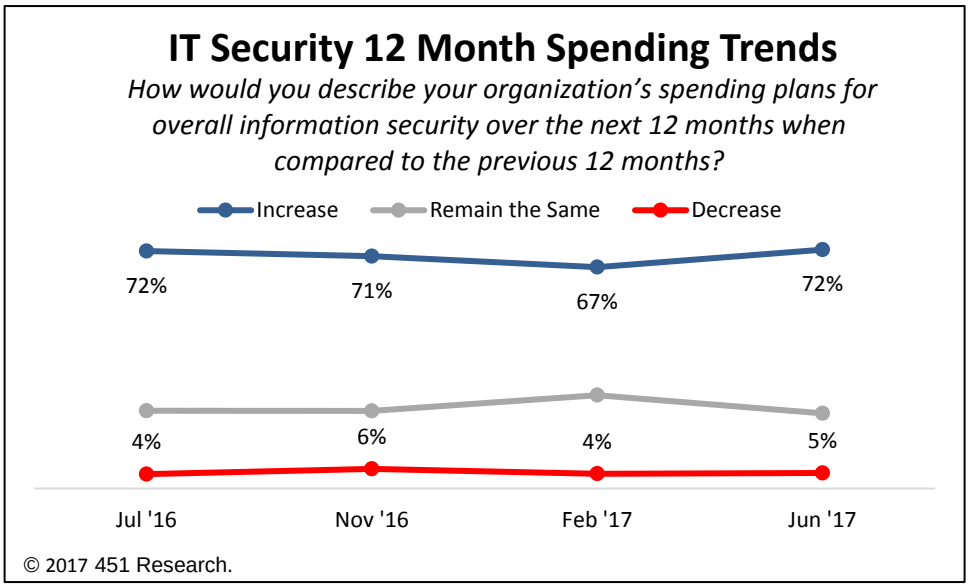
By Tracy Corbo

Information Security Spending Trends

90-Day Spending. A total of 52% of respondents say their organization's information security spending will increase over the next 90 days – up four points from the previous survey in February 2017. Only 3% say spending will decrease, a one-point improvement from the previous survey.



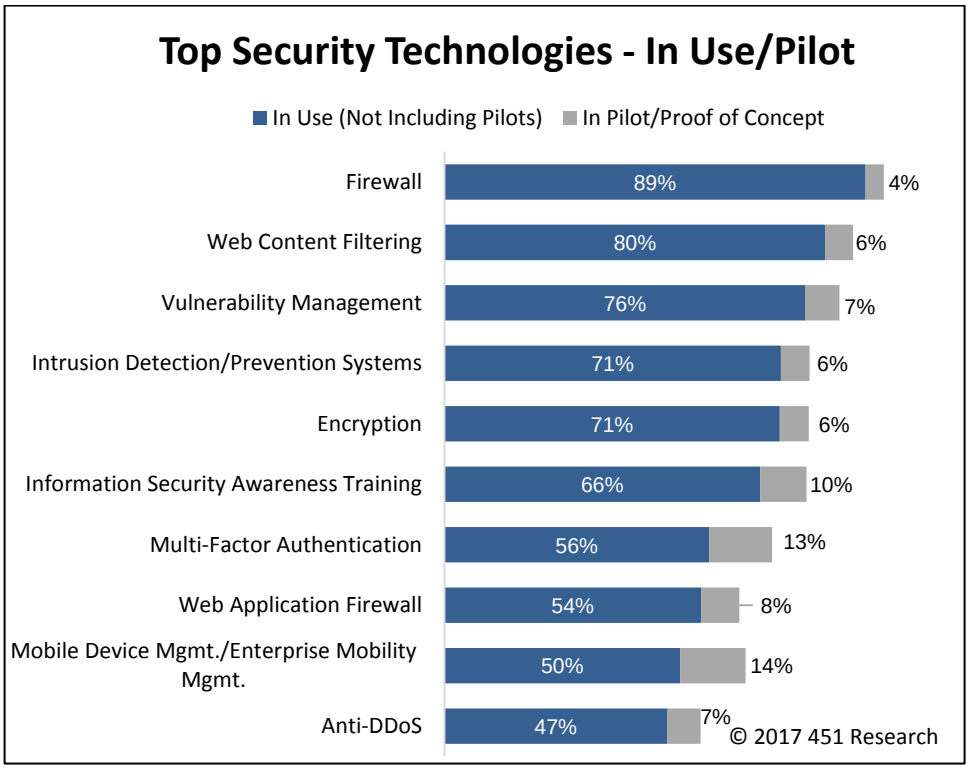
12-Month Spending Trends. Looking at IT security spending plans over the next 12 months indicates that security spending remains strong; 72% of respondents expect a spending increase, up five points from 67% in the previous survey.



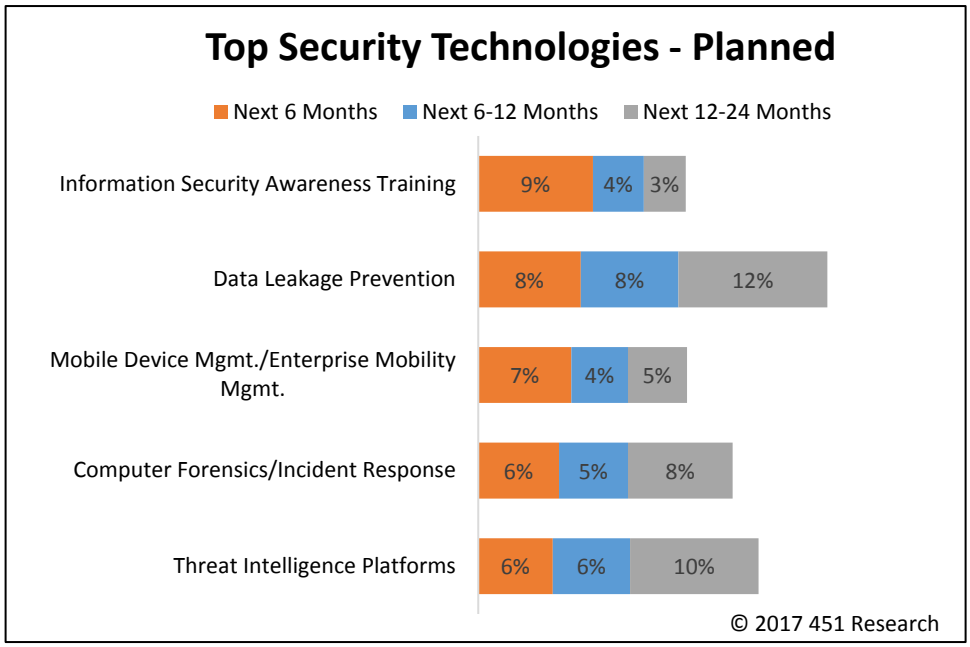
Only 5% say spending will decrease, which is up one point from the February survey.

Security Technology Implementation Status

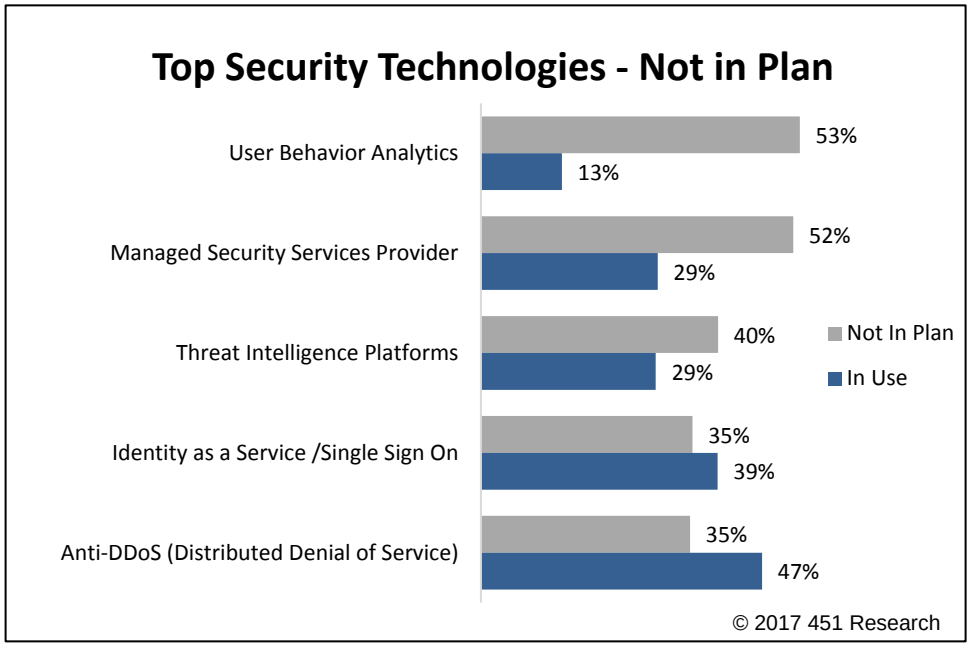
In Use/Pilot. *Firewall* (89%) and *Web Content Filtering* (80%) are the two most widely adopted security technologies in use. Just over three-quarters of the respondents use *Vulnerability Management* (76%) solutions.



Planned. Over the next six months, *Information Security Awareness Training* (9%) tops the list for planned deployments over the next six months. While *Data Leakage Prevention* (8%) is second over the next six months, but that number jumps to 12% over the next two years.

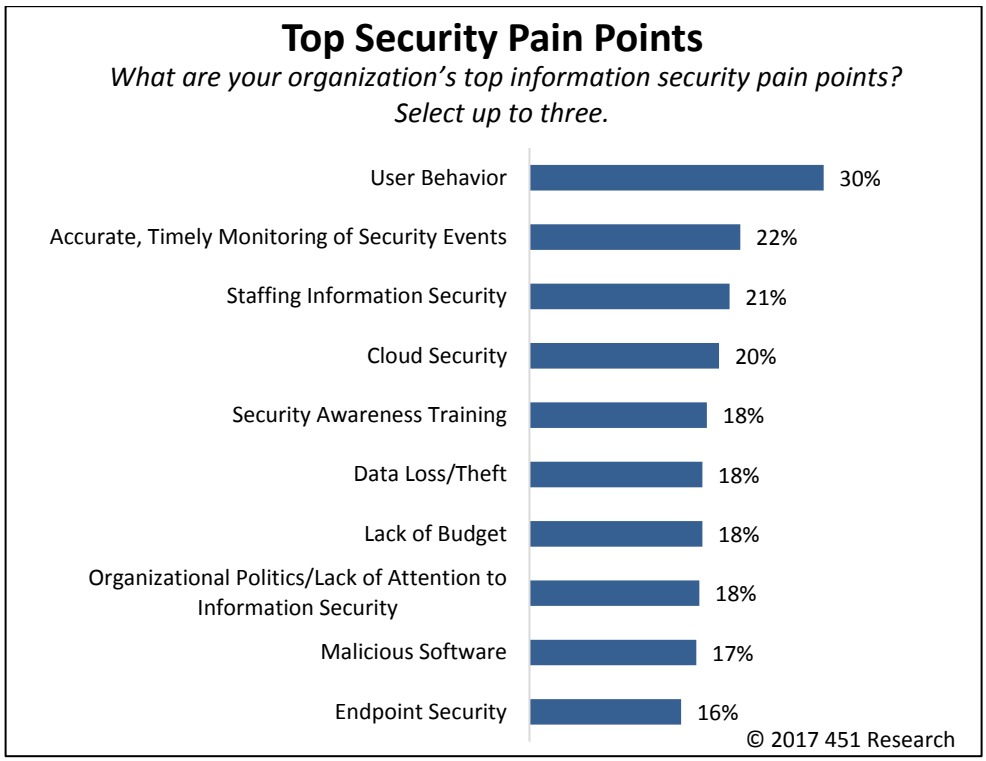


Not in Plan. Only 13% of respondents are currently using *User Behavior Analytics* and just over half (53%) have no plans to implement. While 29% of respondents are currently using *Managed Security Services Providers,* 52% have no immediate implementation plans.

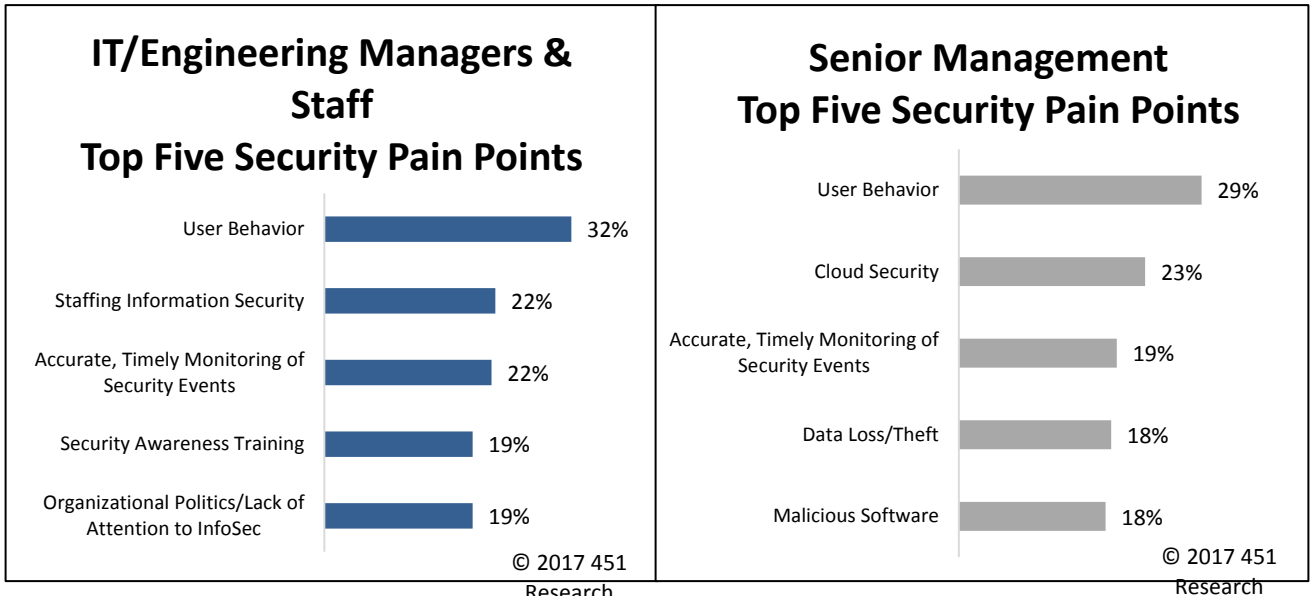


Security Pain Points and Concerns

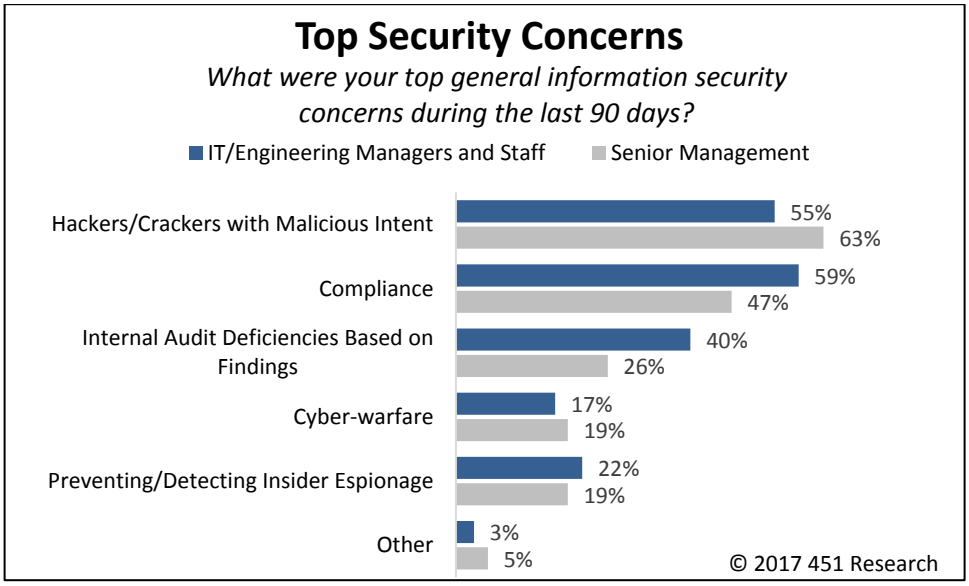
Pain Points. Respondents were asked to select the top security pain points, and *User Behavior* (30%) is the biggest pain point followed by *Accurate, Timely Monitoring of Security Events* (22%) and *Staffing Information Security* (21%).



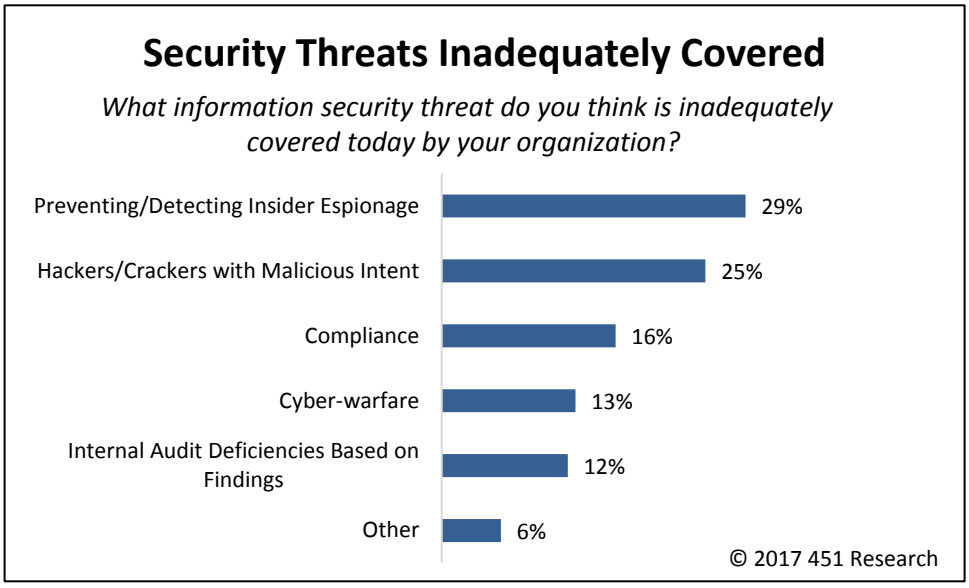
A closer look at the top pain points for IT staff compared to senior management shows that while *User Behavior* is a top concern for both groups, other issues such as *Cloud Security* (23%) is of greater concern for senior management while *Staffing Information Security* (22%) is a top concern for IT staff.



Top Security Concerns. The top security concern over the last 90 days is *Hackers/Crackers with Malicious Intent.* It is of greater concern for senior management (63%) while *Compliance,* the second general security concern, is of greater importance for IT staff (59%).

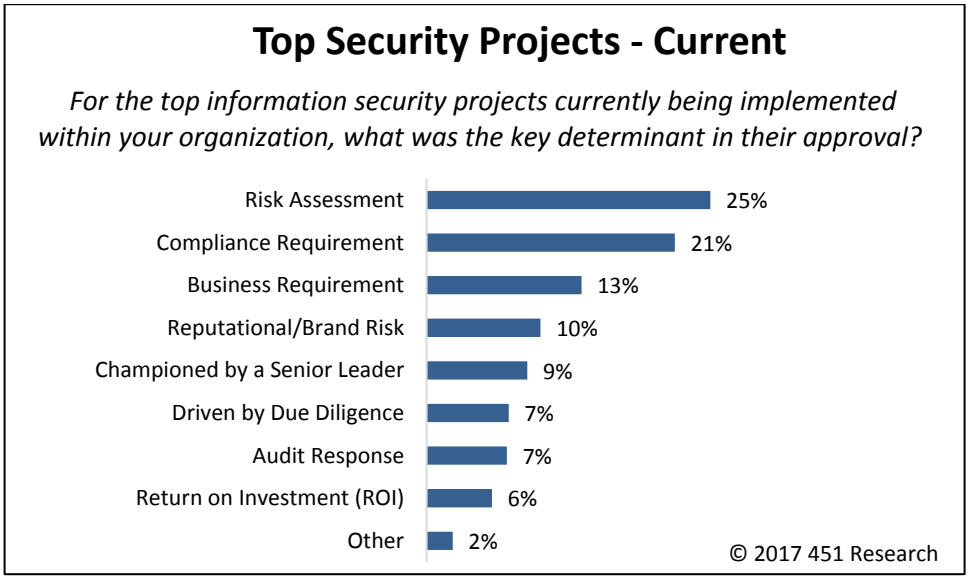


Inadequately Addressed Security Threats. Respondents were also asked which security threats they believe are currently inadequately addressed within their organization. The internal problem of *Preventing/Detecting Insider Espionage* (29%) and the external threat from *Hackers/Crackers with Malicious Intent* (25%) continue to be major security threats.

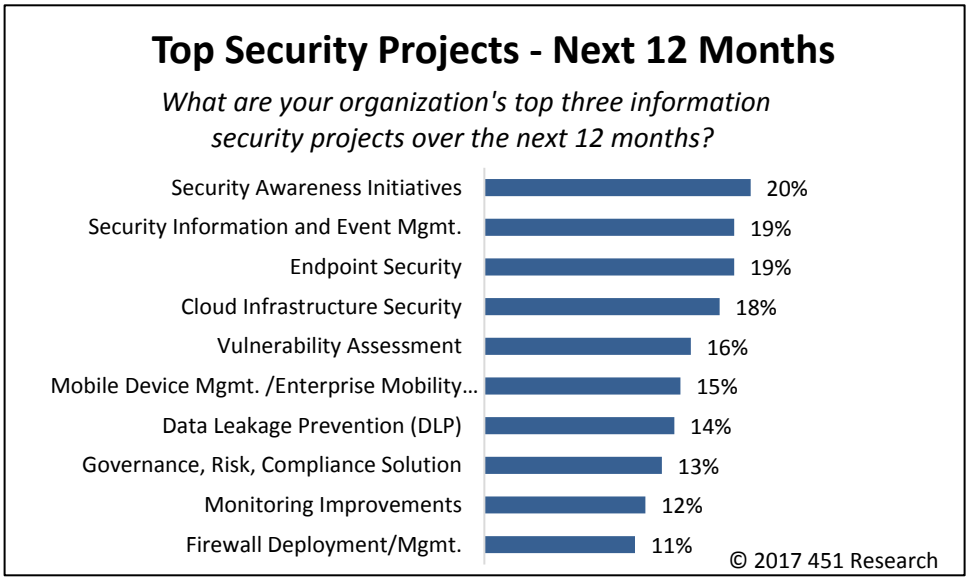


Security Projects

Current. In terms of the top information security projects that are currently being implemented, *Risk Assessment* (25%) and *Compliance Requirement* (21%) are the most popular, followed more distantly by *Business Requirement* (13%).



Next 12 Months. Looking ahead at the top security projects over the next 12 months, *Security Awareness Initiatives* (20%) is slightly ahead of *Security Information and Event Mgmt*. (19%) and *Endpoint Security* (19%), which are both tied for second. *Cloud Infrastructure Security* (18%) is a close third.



Appendix: Security Technology Definitions

Anti-DDoS	Or DDoS Mitigation is typically a bundle of techniques to resist or mitigate the effects of a Distributed Denial of Service (DDoS) attack.
Cloud Access Security Brokers (CASB)	Security policy enforcement points for cloud based applications to holistically manage access and relevant security policies including, for example, authentication, encryption, data leakage prevention, logging, monitoring, and tokenization.
Cloud Infrastructure Security	Any number of a host of software defined security solutions specifically designed to provide security capabilities in cloud virtualized environments.
Data Leakage Prevention (DLP)	Both the name for a strategy to ensure sensitive information is not leaked outside from trusted networks as well as the name for software products that allow an administrator to control what data users can transfer and how.
Dynamic/Static Application Security Tools (DAST/SAST)	Software that is used to search for security vulnerabilities in an application, either by inspecting the source code directly or by running the application from the outside as an external attacker would.
Endpoint Security	Any of a set of solutions including anti-virus, anti-spyware, personal firewalls, application control, host intrusion detection, and antimalware techniques including behavioral blocking or anomaly detection used to protect endpoints (PC's, laptops, mobile devices, servers) on a network by detecting, protecting, remediating, or aiding in the investigation of attacks.
Hosted Private Cloud	Infrastructure deployed with a hosting provider but not shared with other customers and configured for resource pooling, automation and orchestration. May also include self-service, catalogs, metering and chargeback.
Identity as a Service (IDaaS)	An authentication system built, hosted, and managed by a third party provider, generally to provide single or reduced sign on for cloud based services.
Information Security	The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Infrastructure as a Service (IaaS)	Multi-tenant infrastructure shared with other customers and configured for resource pooling, automation and orchestration. May also include self-service, catalogs, metering and chargeback.
Intrusion Detection/Prevention Systems (IDS/IPS)	Network security appliances that monitor network links for potential malicious activity and either alert or alert and block on that activity.
Mobile Device Management (MDM)	Administrative tools for monitoring and managing access of mobile devices including smart phones and tablets.
Private Cloud, On-Premises	Infrastructure in your datacenters that is configured for resource pooling, automation and orchestration. May also include self-service, catalogs, metering and chargeback.

Secure or Protected Enclaves	Subdividing an internal network in such a way that a network has internal protections between differing network zones.
Security Information and Event Management (SIEM)	Technology providing real time analysis of security events or information gathered from logs generated by hardware and applications.
Single Sign On (SSO)	Authentication scheme where a single successful authentication can be used to access multiple distinct applications.
Software Defined Perimeter (SDP)	An extension of traditional fixed perimeter security functions but with a deployment model that allows for flexible deployments in, for example, cloud environments.
Software Defined Security (SDS)	Security components or tools abstracted from specific physical devices (e.g. a specialized security server), designed largely to work within a virtualized infrastructure.
Software-as-a-Service (SaaS)	Consumer applications accessed over the Internet. All aspects of the application are managed by the provider including security, availability, performance, development and maintenance.
Threat Intelligence Platforms (TIP)	A system built around the correlation of external threat data with internal sources to identify and respond to potential security threats.
User Behavioral Analytics (UBA)	Systems designed to provide insights based on the collection and analysis of patterns of user data from data logs.
Vulnerability Assessment	Tools that assist in the identification, quantification, and prioritization of vulnerabilities within a system.

The 451 Global Digital Infrastructure Alliance is a group of highly qualified enterprise technology and IT professionals who work in leading companies of select industries. The Global Digital Infrastructure Alliance regularly surveys its members on a range of business and IT topics, and converts the information into proprietary quantitative and qualitative reports.

451 Research, a division of The 451 Group, is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide 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.