451 Research | Business Impact Brief

Security threats are an inside job

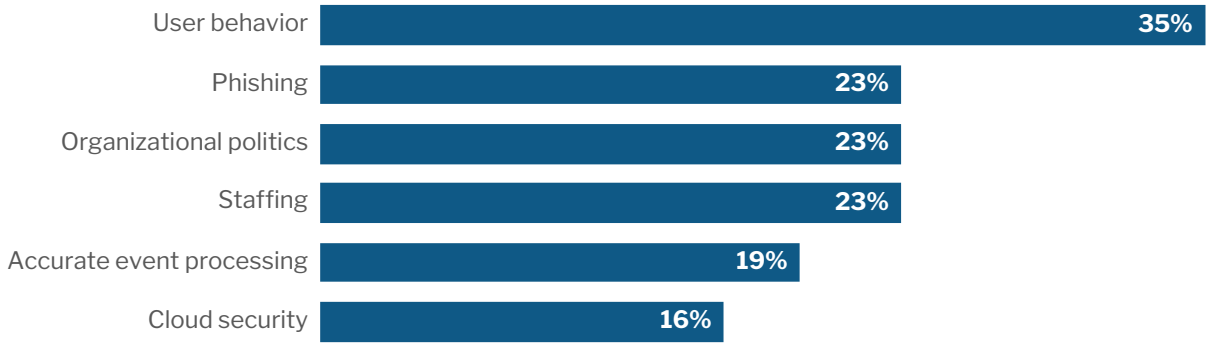
The 451 Take

We spend a lot of time fighting external hackers and glorifying the techniques they use to steal our most sensitive data. But it turns out that the greater pain point for security is user behavior, or what we often refer to as the insider threat. Security teams are finding that a renewed focus on the insider threat – whether hackers compromising insider accounts, privileged users acting with malicious intent, or good people simply making mistakes – is reducing the risk of data loss, costs derived from damages and recovery, and business disruption. We find this to be as true in midsized organizations as it is in large enterprises, as shown in the figure below. Attention to the insider threat promises to yield security benefits not only against attackers, but also in helping employees make better use of IT services.

User Behavior Dominates Top Three Pain Points in Info Security

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2019

Q: What are your organization's top information security pain points?



What is the insider threat?

The insider threat takes multiple forms, each requiring security teams to take a different approach to combat it. Security tools that have elements of machine learning to analyze user behavior, access patterns for sensitive data, servers and external web site domains are essential.

- **Compromised insiders.** A critical milestone for hackers who have penetrated the network is to gain control of user accounts. Once they have achieved that milestone, the hackers become insiders by impersonating legitimate users with the ability to access networked resources and pilfer sensitive data. Security responses to compromises, such as step authentication challenges and isolating insider devices, should be swift to shut down unauthorized access to valuable data.
- **Malicious insiders.** Though rare, nearly every business has experienced users abusing IT operating privileges. Typically, disgruntled employees or those that may be flight risks squirrel away corporate data that may have value for them in their new careers. While security technology certainly looks to stop malicious users in their tracks, the problem often turns into an employee management issue. Machine lerarning security tools trained to detect harmful behavior give management the visibility and activity timelines necessary to resolve issues with malicious insiders.
- **Negligent insiders.** By far the most common class of insider threats are users that just make mistakes or exercise poor judgement and wind up creating security incidents. There are a wide range of examples, from users succumbing to clever phishing attacks, using outdated software that should long since have been updated, or trusting application software that they just pulled down from the web. This is a situation for a kinder, gentler security approach to help negligent users understand their lapses and actively help them do their jobs more securely. Security teams are embracing security awareness programs, for everyone from boardroom executives to backroom consultants, to help educate users and ward off negligence.

451 Research | Business Impact Brief

The 451 Take (continued)

The insider threat is not simply the province of large enterprises in regulated industries; rather, companies of all sizes in all verticals can fall prey to insider threats. In fact, organizations that are heavily distributed, with relatively high levels of workforce attrition and employee access to valuable data – such as those in the retail and hospitality industries – are often first movers with insider threat programs. A common trait is easy access to data that can be used for monetary gain or to meet personal goals.

In many ways, sensitive data is the currency of the organization. We find that data loss, confidentiality, and access control and auditability are leading concerns of organizations embracing cloud hosting services, and that these same issues drive insider threat programs. 451's research into cloud hosting and management shows that 62% of enterpises are moving toward a hybrid IT environment that leverages both on-premises systems and off-premises cloud/hosted resources in an integrated fashion. This places extreme demands on locating where sensitive data is and ensuring the data remains secure. Insiders may change configurations, but the goal inevitably comes down to accessing sensitive data.

Business Impact

Fortunately, there are useful technologies to help secure the business against risks from insider threats:

DATA LOSS PREVENTION (DLP), deployed in the network and on user devices, gives operations visibility into the movement of sensitive data and can block inappropriate access. The ability of DLP products to make data-driven decisions is critical to reducing risks associated with insider threats.

CLOUD ACCESS SECURITY BROKERS (CASB), including those provided by service providers, help monitor insider use of cloud-based resources. CASB gives security personnel important visibility into insider activity, especially with data residing in the cloud.

BEST-OF-BREED ENDPOINT SECURITY TECHNOLOGY HELPS ENFORCE LEAST PRIVILEGE POLICIES. Compromised insiders attempt to escalate privileges to copy data not normally accessed, and negligent insiders often use higher privileges than necessary, leaving security gaps. Proactively managing privilege levels can help manage the insider risk without causing undue user friction.

Looking Ahead

Businesses have a challenge when it comes to designing responses to compromised, malicious and negligent insiders. Differentiating between normal business activity and negligent insiders is one reason why 'data analytics tools and platforms' and 'artificial intelligence/machine learning' are the top two IT priorities this year, according to 451 Research's Voice of the Enterprise: Digital Pulse, Budgets and Outlook 2019. Fortunately, the fundamentals of detection by analyzing access patterns and data usage are consistent across the major insider threat scenarios. We look forward to the day when user behavior is no longer a top pain point for security practitioners. With attention to the insider threat, that day may not be far off.