Privileged Account Exploits Shift the Front Lines of Cyber Security

Contributors
Cisco Talos Security Intelligence and Research Group
Deloitte Financial Advisory Service LLP – Computer and Cyber Forensics Team
Deloitte & Touche LLP – Cyber Risk Services
Mandiant, a FireEye Company
RSA, The Security Division of EMC
Verizon RISK Team, Verizon Enterprise Solutions
The top global firms in cyber threat investigations have identified a common link in today’s most dangerous, targeted attacks and information security breaches: the exploitation of privileged accounts.

Such accounts grant extensive control over sensitive data and IT systems. They’re pervasive in every organization, they’re often overlooked, and they can be powerful weapons in the wrong hands. Now, leading security experts report that privileged accounts are widely abused in targeted cyber attacks and that privileged account exploits have grown increasingly sophisticated.
Information security experts know that the battleground for securing their organizations has shifted. No longer is the battlefront at the network perimeter; it’s within the enterprise, inside the network. For most large corporations and governmental organizations, infiltration by cyber adversaries is persistent – almost a given. This grave reality prompted then-FBI Director Robert Mueller to make this statement in 2012: “There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.”

Ninety percent of organizations surveyed in a Ponemon Institute study said they had experienced at least one breach, with 59 percent of respondents claiming two or more breaches within a year’s time. Cyber attacks have become not only commonplace – disclosures from Home Depot, JPMorgan Chase, Kmart, Staples and Target are recent examples – but they also take a tremendous economic toll:

- Malicious cyber activities cost organizations worldwide US$300 billion to US$1 trillion in losses annually.
- Malicious or criminal cyber attacks are the most common cause of data breaches worldwide, accounting for 42 percent of data losses. Cyber attacks also cause the most costly types of data breaches, amounting to US$159 per capita worldwide in losses.
Companies worldwide spent an average of US$3.5 million in 2013 to investigate, remediate and notify affected parties of each security incident, a 15 percent increase from 2012.  

The United States alone may have lost more than a half-million jobs from cyber espionage and crime.  

In the spectrum of malicious cyber attacks, the greatest threats—and the most serious information losses—typically result from targeted attacks, complex hacks that are custom-designed to infiltrate the high-value data and technology systems of corporations and governmental entities. Because targeted attacks take advantage of a specific organization’s weaknesses, finding attack patterns that fit a broad range of cases is difficult. But there is one pattern that can be found in almost all targeted attacks: the exploitation of privileged accounts. 

Privileged accounts ship with every piece of information technology, including servers, desktops, applications, databases and network devices. The accounts confer powerful controls to IT administrators. Other types of privileged accounts grant restricted user groups special access to sensitive business functions. For instance, the accounting department may have privileged access to restricted financial data, and monitoring applications may have unrestricted access to a wide range of databases. Privileged accounts provide considerable leeway to authorized employees and machines needing to perform specialized functions. Because of the power and freedom invested in these high-level types of accounts, they can be lethal in the wrong hands.
Privileged Accounts Exploited in Cyber Attacks

New research commissioned by cyber security firm CyberArk finds that privileged accounts are exploited in the vast majority of targeted attacks. Using such accounts, attacks can proceed faster, easier and with lower risk of detection. Privileged accounts even enable attackers to destroy evidence of their activities and establish redundant access points and backdoors that make it nearly impossible to keep them off internal networks.

While most targeted cyber attacks are not publicly disclosed, CyberArk commissioned research to uncover how such attacks are conducted by interviewing top firms that investigate and remediate cyber attacks for Global 1000 companies. The firms interviewed were Cisco Talos Security Intelligence and Research Group; Deloitte & Touche LLP’s Cyber Risk Services; Deloitte Financial Advisory Service LLP’s Computer and Cyber Forensics Team; Mandiant, a FireEye Company; the Advanced Cyber Defense team at RSA, the Security Division of EMC; and the Verizon RISK Team of Verizon Enterprise Solutions. Interviews with these firms provided insight into the extent to which privileged accounts are compromised and exploited in targeted cyber attacks, even incidents that are not publicly reported. Here are key findings from CyberArk’s research interviews:

1. **No one is safe**: every company is now a potential target. Cyber attackers have broadened their targets, attacking companies of all sizes in a broad range of industries. Cyber threat investigators have even seen attackers targeting companies simply as a means to gain trusted access to their supply chain partners.

2. **Attackers will get in**: the most likely point of infiltration is via an organization’s employees. Phishing attacks are increasingly sophisticated, making employee log-ins far easier points of infiltration than network or software exploits.

3. **Attackers typically stay hidden inside the enterprise for months and even years.** Cyber investigations experts discover that most attacks have been ongoing for 200 days or more before finally being detected. Monetary attacks usually have a much shorter time to detection, usually less than 30 days. Attackers use various methods to cover their tracks, but a common technique is to use privileged accounts to delete log data and other evidence of illicit activity.

4. **Attackers covet privileged access**: privileged accounts are exploited in almost all targeted cyber attacks. Top security incident response firms claim that between 80% to all of the serious security incidents they investigate compromise and misuse privileged accounts at some point in the attack process.

5. **Privileged accounts are vastly underestimated**: the risks and security vulnerabilities posed by privileged accounts are much larger than most companies realize. The cyber threat investigators interviewed for this report believe companies tend to underestimate the dangers posed by compromised privileged accounts. CyberArk’s research indicates that organizations today have at least 3- to 4 times as many privileged accounts as employee headcount.

6. **Attackers show increasing sophistication in exploiting privileged access**: they’re using privileged accounts to break into a wider range of systems and to become harder to dislodge from networks. Security investigators report a range of privileged account exploits, from hacking embedded devices in the Internet of Things to establishing multiple privileged identities in Microsoft Active Directory to ensure redundant points of access.
Finding #1: **No one is safe**

It used to be that unless you were a bank, credit card processor or manufacturer of military weaponry, cyber attackers wouldn’t bother to home in on you. Now, no one is safe. “Every company has something of value to protect, something that attackers want. In today’s connected business world, everyone is a potential target,” said Craig Williams, a top security researcher at Cisco Talos Security Intelligence and Research Group.

The cyber threat investigators interviewed for this report say that attackers have expanded their sights to include companies in retail, media, energy, manufacturing and IT services, among others. Companies are chosen as targets of cyber espionage or for financial gain through monetization of stolen data. In some cases, however, the companies being attacked are merely a means to an end: attackers are after their supply chain partners.

For example, one security investigator described a cyber attack against a major manufacturer of pipes and plumbing parts. Forensic evidence suggested the attackers breached the IT systems of the pipe manufacturer to collect information on the company’s customers. Through sales invoices, they could learn what type and size of tubing had been purchased for specific customers’ pipelines and oil rigs. The attackers also appeared to be looking for opportunities to infiltrate the supply chain management systems of the pipe maker’s business partners, in particular a prominent home improvement chain.

The IT systems of small- and mid-sized companies are presumed to be less sophisticated and their security defenses easier to infiltrate. Threat investigators observe that cyber attackers will often target such companies for the access they have to the corporate networks of larger, more secure business partners. For this reason, threat investigators have traced attacks to non-traditional targets such trucking companies and all types of professional services firms, from management consultants and auditors to litigation attorneys.
Finding #2: Attackers will get in

Cyber threat investigators agree that it’s probably not possible to stop determined, skilled cyber attackers from getting inside enterprise networks. In targeted attacks, adversaries do extensive research and reconnaissance of their victims’ IT environment and security tools. They will look for unpatched software, improperly configured servers or any other technical vulnerability to gain entry.

In rare cases where a deficiency cannot be found, attackers can customize malware code so it can circumvent anti-virus software, firewalls and other perimeter security tools. When all else fails, attackers can exploit a rare “zero day” vulnerability, an undiscovered exposure inherent in an application or computing system.

“Everyone thinks about the zero day vulnerability, but they’re rarely exploited in a widespread pattern in the wild. They’re so valuable that attackers apply them in very limited way,” said Cisco’s Craig Williams. “For every zero day you hear about, there are millions of known vulnerabilities that are far more likely to be used against you.”

Threat investigators report that attackers increasingly gain illicit entry through people, not networks. Infiltration techniques that take advantage of people’s misplaced trust are often easier to execute than exploiting network or software vulnerabilities. “It’s easier to get into the environment by phishing than by brute force attacks or dictionary approaches,” explained Christopher Novak, Global Managing Principal, Investigative Response for the Verizon RISK Team. “Attackers want IT credentials or they target a high-ranking individual within the company. Usually those users are trusted and have relatively unencumbered access. They’re also not closely monitored by IT.”

The cyber threat investigators interviewed for this report have seen phishing and social engineering techniques become increasingly sophisticated and credible-seeming. “If an attacker sends out 20 or 30 phishing emails, there’s a good chance he’ll penetrate your network,” said Christopher Novak of Verizon. “The phishing attacks are that sophisticated. No company is immune from them.”

Peter Tran, the incident response lead from RSA, provided a detailed example: “We’ve set up fake online personas, pretending to be a PhD researching cancer therapies or an engineer developing a new laser module for a defense system. It’s a social media honeypot designed to attract an advanced adversary. We see what type of inquiries we get and learn their techniques... And what we’re seeing is attackers have gotten really good. They’re masquerading as recruiters and reaching out to high-value targets such as senior engineers, business managers. They use social media to start dialogs with valuable insiders, and they take time to cultivate relationships. Based on what we’ve seen, [attackers are] credible enough to fool most people into providing the entry point they need.”
Finding #3: **Attacks stay hidden for months or years**

The cyber threat investigators interviewed for this report often find evidence that cyber attacks have been ongoing for months and even years before they’re discovered. Investigators estimate it takes an average of six to eight months before their clients detect a problem and call for help. This time estimate is consistent with Mandiant’s published findings, which peg the median number of days attackers were present on clients’ networks at 229 before discovery.⁶

Threat investigations teams have seen attacks go on for years before discovery, as long as seven years, according to one of the experts interviewed. A common reason why cyber attacks go undiscovered for so long is that victim organizations don’t proactively look for problems. Why should they when they don’t see themselves as desirable targets? “We found that a grocery store chain had an infiltrator in their supply chain for years. Part of the problem was denial: they never thought they would ever be anyone’s target,” said Peter Tran of RSA. “But attackers these days aren’t just trying to get payment cards; they’re looking for business information. Details about how you run your business, trade secrets on how you’ve improved supply chain efficiency can be incredibly valuable and important.”

In many cases, companies that have been attacked don’t discover the data breach themselves. “In probably a number of the cases we get involved in, it is the FBI or other federal agencies notifying the company that they have gotten their data from an exfiltration site,” said incident response specialists from Deloitte. Similarly, Mandiant’s threat research found that only one-third of security breaches in 2013 were identified by attacked companies; the other two-thirds were notifications from external parties.⁷

“Companies don’t realize they’re under attack, because no alarms were triggered by all the security tools they’ve deployed,” explained RSA’s Peter Tran. “The attackers circumvent your detection mechanisms. You’ll never find them in time (to stop damage) if you wait for SIEM alerts; you’ve got to proactively hunt for them.” Hunting down hidden threats requires organizations to learn what patterns of behavior are typical and accepted for their users, both human and machine. Then, security teams need to spot deviations from accepted norms and analyze whether anomalous behaviors indicate illicit activity.

In most cases of persistent infiltration – instances in which attackers try to prolong their hidden presence within a network – cyber criminals go through great pains to hide their tracks. “In targeted intrusions, most attackers don’t install malware on the majority of systems they compromise. They don’t want to leave unnecessary tracks,” said Jim Aldridge, an investigation lead for Mandiant. “Plus, if they already can access the network at will to get privileged access to a system, they don’t need to install a backdoor. They can come and go when they need to. Malware just leaves a trail that might make them easier to find. The goal is to stay low, look like any other legitimate user in the system. One attack we investigated only involved one system infected with a backdoor, but it only takes one vulnerability for you to lose valuable data... It’s much harder for attackers to do that without privileged access.”

---

Finding #4: **Attackers covet privileged access**

Cyber threat investigators report that privileged accounts are a favored avenue of criminals conducting targeted cyber attacks and other malicious cyber activities. The security specialists interviewed estimate that between 80% to “almost all” of the serious cyber attacks they’ve investigated exploit privileged accounts at some point in the attack process.

“Almost all targeted attacks to which I’ve responded have involved the attacker obtaining some form of privileged access,” said Jim Aldridge of Mandiant. “Attackers want to get their hands on privileged accounts because they’re the easiest way to enable lateral movement. They could penetrate internal systems by exploiting unpatched software vulnerabilities, which are inevitably present, but using a privileged log-in saves them a lot of effort and time. They use the legitimate credentials to help them reach systems that contain the data they want, starting from their initial points of entry into the network. Once they get access to an internal system, privileged accounts let them move internally to other systems much faster and easier and with lower risk of detection.”

The compromise and misuse of privileged accounts is one of the few patterns common among targeted cyber attacks. Threat investigators from Deloitte explained: “Privileged accounts are a hall pass that can get attackers where they want to go without constraints. It enables them to traverse the network without hindrances. … Most times, [attackers are] looking to exfiltrate data, and once they have privileged credentials, they are pretty much home free. They can hide their tracks so you cannot easily detect or stop them. When the attackers get privileged access, the kill chain concept is done.”

Threat investigation experts equate illicit access to privileged accounts to gaining:

- **A hall pass**
- **The golden ticket**
- **Keys to the kingdom**
- **An all-access pass**
- **The skeleton key for IT**
Finding #5: **Privileged accounts are vastly underestimated**

Because privileged accounts are frequently exploited in cyber attacks, threat investigators say it’s imperative that companies know what users have access to what types of sensitive data and IT systems. Tracking and monitoring privileged accounts can be challenging, given the complexity of many enterprise IT networks and the proliferation of corporate data and applications in cloud, mobile and social environments.

The threat investigators interviewed for this report say that many companies don’t have an accurate inventory of their information “crown jewels” or which employees and technology systems have privileged access to these prized data assets. In fact, many organizations probably don’t know how many privileged accounts they have and on what systems they reside. As organizations continue to add to their IT infrastructure, the number of privileged accounts grows organically. Data from CyberArk suggests that most organizations, as a rule of thumb, have at least 3x to 4x as many privileged accounts as employees.

Many privileged accounts are provisioned for machines, not people. IT departments set up “service accounts” to enable machine-to-machine access to software applications and computing equipment. To minimize the risk of broken interdependencies among systems, IT administrators often give service accounts broad access privileges, sometimes even the ability to connect to any computer in the enterprise, not just the systems to which the account is required to connect. These conditions have contributed to a proliferation of privileged accounts that often go unmonitored or are sometimes even forgotten.
“Most companies expect service accounts to be used only internally, so they keep the default passwords,” he continued. “We’ve seen 25 or 30 attacks recently in which attackers used (publicly available) default passwords. Also, account lockouts are usually turned off for service accounts to prevent breakdowns in dependencies between systems. And because it’s presumed individuals aren’t using [these accounts], analysts dial down the sensitivity on alerts. Service accounts are out of sight, out of mind. So, if a threat actor gets into the environment and enumerates the service accounts, which is easy to do, they can make a lot of headway very quickly with low risk of discovery. Service accounts aren’t restricted to communicating with only certain systems, and some have domain admin privileges. Attackers can use them to set up data exfiltrations and to create secondary or tertiary backup accounts (to create persistence).”

Attackers are also exploiting privileged access to a broader range of machines. The Cisco Talos Security Intelligence & Research Group recently uncovered an unusual exploit dubbed the Zollard Worm. The worm adapts malicious binary code to run on a range of non-PC or “embedded” devices built on different computing architectures. Zollard executes in a browser outside of normal directories, meaning it has privileged access to system resources. Its goal? To commandeer the processing power of DVRs to mine for bitcoins.

The significance of the Zollard Worm is that it marks a privileged account hack on non-traditional types of Internet-connected devices — what’s increasingly described as the Internet of Things. The variety and volume of electronic devices communicating via the Internet will grow exponentially. Cisco predicts 25 billion devices will be connected by 2015 and 50 billion by 2020. The Internet of Things encompasses new types of critical systems that will inevitably require privileged accounts to manage them, such as heart pacemakers, insulin pumps and home alarm systems — “things” that should never, ever be compromised.

Yet, Cisco and other threat research firms expect the Internet of Things to become increasingly attractive to cyber attackers in the future. Craig Williams explained why:

“Since embedded devices require firmware updates, they typically have more complex quality assurance cycles, which in turn may cause them to lag behind other products from a security update perspective. To complicate this further, embedded devices often have a very basic setup process...”
“Service accounts are out of sight, out of mind. So, if a threat actor gets into the environment and enumerates the service accounts, which is easy to do, they can make a lot of headway very quickly with low risk of discovery.”

that is run once at deployment, and then never touched again. This results in most embedded devices running fairly standard configurations. If a vulnerability is found in default or common embedded configurations, attackers are much more likely to focus on it since the attack surface is going to be widespread.”

In the traditional realm of connected devices, threat investigators have seen cyber attackers focused on escalating their access privileges to compromise Microsoft Active Directory. “It’s not uncommon for all AD passwords to be compromised. Then, they all need to be reset, which is complicated because of service account dependencies,” said Mandiant’s Jim Aldridge.

Even if all user accounts are reset, RSA’s incident response lead has seen instances in which resets of Microsoft Active Directory don’t necessarily work the first or even second time. “Many attackers seek to ‘dump’ or ‘tip’ the Active Directory so they can set up their own credentials and create multiple points of entry to mask their activities,” said Peter Tran. “When Active Directory gets owned by an adversary, clients typically make all their users change their accounts. But that’s done by email, and the adversary will have gained access to email. They’ll read about IT announcing a password change, so they’ll stand by to collect the new passwords. They’ll scan for organizational unit Active Directory accounts and harvest all the records again. So you’re back where you started. We’ve seen that happen multiple times.”

The cyber research team at Verizon helped a large enterprise remediate a service directory hack. A team of hacktivists secured a service account with domain admin privileges. “The attacker reset the passwords for everyone in the company, so all 30,000 employees were calling the IT help desk wondering why they’re locked out,” said Verizon’s Chris Novak. “Imagine your employees having no access to email, trading accounts or anything. And IT couldn’t deal with the volume. They’re accustomed to 100 lockouts a day, not 30,000.”

---

8 Cisco Internet Business Solutions Group. "The Internet of Things Visualization."
Recommendations and Conclusions

Stopping privileged account exploits is often the organization’s last line of defense before a data breach. That’s because once privileged accounts are compromised, attackers gain dangerous levels of access to critical IT systems. Cyber threat researchers point out that once privileged accounts are compromised, it means attackers have already gotten inside the trusted IT environment. They’ve not only gained entry, but they’ve also performed reconnaissance on networks, escalated privileges, established multiple footholds and are now moving laterally to other systems. Observes Jim Aldridge of Mandiant, “At this point, it’s critical to detect attacker movements, because it’s basically the last chance you have before they steal data.”
The security experts interviewed for this report provided some basic guidance to help companies detect and reduce misuse of privileged accounts:

- **Know what privileged accounts you have.** What they do and are supposed to do. Consider IT administrative credentials, default and hard-coded passwords, application backdoors, SSH keys, etc. Then, limit those privileges as much as possible to reduce the potential for abuse.

- **Improve security of privileged accounts** by changing default passwords and using different administrative passwords on each system. If attackers gain privileged access to one system, they usually will try the same password to gain access to all other similar systems within the company. Enforce one-time passwords that expire after a single use. For further protection, companies can encrypt their privileged account credentials and automate credential rotation.

- **Proactively monitor privileged accounts** and how they interact with data and technology assets. Do not passively wait for security tools to alert you of a problem. For example, scout for admin credentials that should not be accessing certain types of systems or for domain admins logging into many different parts of the network. If a privileged user is VPNing into the network from multiple far-flung locations in a short amount of time, that’s often a sign of fraudulent access.

- **Perform regular, recurrent “housekeeping”** of information assets and how they’re accessed. Develop and employ tight governance practices around the provisioning of user access and privileges and around data and asset classification. Scrub your Active Directory and all authentication/access points. Decommission privileged accounts that haven’t been used recently. Many will likely be service accounts with fixed credentials.

- **Monitor and limit the privileges of service accounts.** For example, if an account runs a particularly important service, it should never have remote access. In many cases, it shouldn’t even be usable through a graphical user interface (GUI). For example, a service account running a database should never need a GUI to access its services.

- **Apply patches as quickly as possible.** Many companies worry about zero day vulnerabilities, but such exploits are so valuable that attackers use them only in special circumstances and hardly ever on a widespread basis. For every zero day you hear about, there are millions of known vulnerabilities that can be eliminated through patching.

- **Practice classic defense in depth.** The more overlapping security layers in your environment, the more you lower your risks. Reducing vulnerabilities in privileged accounts can greatly impair the ability of attackers to maneuver within and manipulate critical IT systems.

The collective experiences of the world’s leading threat researchers show that cyber attackers are almost guaranteed to go after privileged accounts. Companies and governmental agencies defending against targeted cyber attacks should take steps to safeguard their many points of privileged access. Securing privileged accounts is the new critical front line of defense for organizations committed to winning today’s battle for cyber security.
Expert Contributors

Cisco Talos Security Intelligence and Research Group
The Cisco Talos Security Intelligence and Research Group (Talos) is made up of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detects, analyzes and protects against both known and emerging threats. Calling on an unrivaled telemetry data set, Talos creates intelligence that provides a holistic understanding of threats translating to leading security effectiveness for Cisco security solutions. Talos is part of the Cisco Collective Intelligence (CSI) ecosystem.

Deloitte
With the proliferation of Internet-enabled devices, cyber culture is growing more rapidly than cyber security. Everything that depends on cyberspace is potentially at risk. Private data, intellectual property, cyber infrastructure, and even military and national security can be compromised by deliberate attacks, inadvertent security lapses and the vulnerabilities of a relatively immature, unregulated global Internet. Working hand-in-hand with clients, Deloitte helps organizations plan and execute an integrated cyber approach to harness the power of information networks to enhance business operations, increase mission performance and improve customer support, without compromising security or privacy.

Mandiant, a FireEye Company
Mandiant has driven threat actors out of the computer networks and endpoints of hundreds of clients across every major industry. We are the go-to company for the Fortune 500 and government agencies that want to defend against and respond to critical security incidents of all kinds. The majority of advanced targeted operations proceed undetected and proliferate undefended. When intrusions are successful, Mandiant’s unique combination of human intelligence and technology leadership, combined with threat intelligence from FireEye, help organizations detect, respond to and contain them before the threat actors reach their objective. Our engineers and security consultants hold top government security clearances, have written 11 books, and are regularly quoted by leading media organizations. Mandiant is headquartered in Alexandria, VA, with offices in New York, Los Angeles and San Francisco.

RSA, The Security Division of EMC
RSA, The Security Division of EMC, is driven by its uncompromising belief that organizations should not have to accept getting breached or hacked as an unavoidable consequence of communicating, collaborating and innovating in a digital world. In fact, every day, and for over 30 years, RSA’s singular mission has been to help our more than 30,000 customers around the world protect their most valuable digital assets. RSA believes that organizations must become aggressive defenders of their right to operate securely and that no other company is in a better position to help them.

RSA’s Intelligence Driven Security solutions help organizations reduce this risk. Through visibility, analysis and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cyber crime. With Intelligence Driven Security, organizations no longer have to take a “wait and let’s see what happens” approach to security.
Verizon Enterprise Solutions, Global Managed Security Solutions

Verizon is a leader in delivering global managed security solutions to enterprises in the financial services, retail, government, technology, healthcare, manufacturing, energy and transportations sectors. Verizon combines powerful intelligence and analytics with an expansive breadth of professional and managed services, including customizable advanced security operations and managed threat protection services, next-generation commercial technology monitoring and analytics, rapid incident response and forensics investigations and identity management. Verizon brings the strength and expert knowledge of more than 550 consultants across the globe to proactively reduce security threats and lower information risks to organizations.

ABOUT THE REPORT’S SPONSOR

CyberArk (NASDAQ: CYBR) is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world’s leading companies — including more than 35 percent of the Fortune 100 and 17 of the world’s top 20 banks — to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific.

For more information on this report, please visit: www.cyberark.com/contact or call +1 (617) 965-1544.