How Well is Your Organization Protecting its Real Crown Jewels - Identities?

INSIDE
- Complete Survey Results
- Expert Analysis
- Insights from Hitachi ID Systems CTO Idan Shoham
Do you have confidence in your organization’s ability to manage privileged identities and prevent their abuse?

Can your security team detect and identify intruders before data disappears?

Are you confident that former employees and contractors no longer have access to your critical systems?

These are among the questions we set out to answer in the 2015 Privileged Access Management Study, sponsored by Hitachi ID Systems, and the responses help create an eye-opening information security agenda for 2016.

More than 90 percent of survey respondents are concerned about external and/or internal attackers gaining unauthorized access and compromising corporate networks. And the survey results offer sound reasons for these concerns:

• 47% of respondents believe that former employees, contractors or vendors are still familiar with their organization’s processes to change passwords on shared accounts;
• Only 42% have deployed a multifactor authentication technology for high-risk or highly privileged users;
• Only 40% have deployed automation to control access to shared, privileged accounts.

This study was designed to examine just how well organizations are protecting their true crown jewels – identities. In this report, you will receive survey results that explore:

• How organizations are best managing privileged identities;
• The true business impact of intrusions due to external/internal privileged users;
• Modern methods being employed to detect both accidental and malicious activity.

This survey was conducted online during the fall of 2015, and we had more than 130 respondents from organizations across global regions and industry sectors.

Join me in a review of the full survey responses, and then let’s discuss how you can put this data to use to help improve your organization’s capabilities to protect identities and privileged access.

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com
About this survey:
This study was conducted online during the fall of 2015. More than 130 respondents participated internationally from organizations of all sizes and across industries, with concentrations of respondents in the financial services and healthcare sectors.

Table of Contents

Introduction ................................................................. 2
Big Numbers ................................................................. 4
Survey Results ............................................................... 5
  I. Baseline ................................................................. 5
  II. External Intrusions .................................................. 6
  III. Internal Abuse ....................................................... 9
  IV. Existing Processes .................................................. 11
  V. Infrastructure ........................................................ 13
  VI. The Cost of Security ............................................... 15
  VII. 2016 Agenda ......................................................... 17

Conclusions ................................................................. 19
Survey Analysis ............................................................. 20
  Idan Shoham, CTO, Hitachi ID Systems.

Resources ................................................................. 25

Sponsored by

Hitachi ID Systems delivers access governance and identity administration solutions to organizations globally. Hitachi ID solutions are used by Fortune 500 companies to secure access to systems in the enterprise and in the cloud. To learn more about Hitachi ID Systems, visit Hitachi-ID.com
Big Numbers

Some stand-out figures from this survey.

53%
Rate as above average or superior their organizations’ ability to manage privileged identities and external/internal access to critical systems.

96%
Say they are somewhat or very concerned about outside attackers compromising their corporate networks.

91%
Are somewhat or very concerned about legitimate employees, contractors or vendors abusing their privileged network access.
I. Baseline

In this opening section, respondents were asked to offer a general assessment of their organizations’ abilities to manage privileged identities and access – and where they see their biggest failings. The key takeaways:

- Only 53 percent of respondents rate their organizations at above average or superior
- 23 percent say their Achilles Heel is a failure to enforce existing policies.

Full results to these questions follow.

How do you assess your organization’s ability to manage privileged identities and external/internal access to critical systems and data?

<table>
<thead>
<tr>
<th></th>
<th>Above Average</th>
<th>Average</th>
<th>Below Average</th>
<th>Superior</th>
<th>Failing</th>
</tr>
</thead>
<tbody>
<tr>
<td>46%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At a time when targeted attacks are rampant, and when many of the highest profile data breaches owe to stolen credentials, it’s disconcerting to see that 47 percent of respondents rate their defensive capabilities at average or below.

But what is missing in cybersecurity is a tangible definition of what “average” truly means. Does it mean “just good enough,” or “we’ve been lucky so far?”

Further results will show exactly where security leaders feel most and least confident.

What do you see as your organization’s single biggest failing when it comes to managing privileged identities and external/internal access to critical systems and data?

- We fail to enforce the good policies we have: 23%
- We lack the right technology tools: 22%
- We lack the trained staff to properly manage the tools: 17%
- The organization fails to recognize this as a critical objective: 13%
- We lack financial resources to invest in staff and tools: 9%
- We lack the right policies: 7%

When assessing organizations’ vulnerabilities, three areas stand out: Governance, tools and staffing. Respondents say their organizations often do have good policies for managing privileged identities – they just often fail to enforce them. And while many organizations do lack the proper tools to support their policies, others are stymied by a deficit of trained staff to properly manage the tools.

With these baseline figures in mind, look next at where organizations are vulnerable to external and internal attacks.
II. External Intrusions

In the era of the Sony, OPM and TalkTalk breaches, security leaders are particularly sensitive to the risks of external attackers hacking into corporate networks. In this section, respondents convey:

- 96 percent are somewhat or very concerned about external attackers
- 32 percent say it can take more than 24 hours to detect external intrusions

What is your level of concern about outside attackers compromising your corporate network?

<table>
<thead>
<tr>
<th>Concern Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Somewhat concerned</td>
<td>53%</td>
</tr>
<tr>
<td>Very concerned</td>
<td>43%</td>
</tr>
<tr>
<td>Not at all concerned</td>
<td>4%</td>
</tr>
</tbody>
</table>

No surprise: In the era of the high-profile data breach – where boards of directors and business leaders are held accountable for their organizations’ security lapses – 96 percent of respondents are somewhat or very concerned about the risk of external attackers compromising their networks.

The key follow-up question is: Have their concerns been validated by external intrusions?

In the past 12 months, did your IT organization detect any external intrusions that resulted in unauthorized access to your corporate network?

- 22% Yes
- 78% No

Roughly one-fifth of respondents say their organizations suffered an external intrusion in the past year. But it’s fair to point out: These are the respondents who know their corporate networks were breached. At a time when so many of these attacks are “low and slow” and avoid detection, it’s fair to assume that a fair number of organizations were breached … but do not yet know it.

How long did it typically take your IT organization to detect any external intrusion(s)?

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 24 hours</td>
<td>32%</td>
</tr>
<tr>
<td>Under 60 minutes</td>
<td>30%</td>
</tr>
<tr>
<td>1 to 3 hours</td>
<td>11%</td>
</tr>
<tr>
<td>3 to 6 hours</td>
<td>11%</td>
</tr>
<tr>
<td>6 to 9 hours</td>
<td>9%</td>
</tr>
<tr>
<td>12 to 24 hours</td>
<td>7%</td>
</tr>
</tbody>
</table>
Indeed, when nearly one-third of respondents say it takes more than 24 hours to detect the typical external intrusion, then it is fair to say that many of these attacks are adhering to the “low and slow” approach, giving the attackers more opportunity to gain access and exfiltrate data.

How long did it typically take your IT organization to stop any external intrusion(s)?

- Under 60 minutes: 36%
- 1 to 3 hours: 23%
- 3 to 6 hours: 5%
- 6 to 9 hours: 10%
- 9 to 12 hours: 3%
- 12 to 24 hours: 3%
- More than 24 hours: 15%
- We did not stop the external intrusion: 5%

It is encouraging to see that – once detected – external intrusions often are stopped in under one hour – or within one to three. But, again, it’s worth reinforcing that the attacks have to be detected before they can be stopped. And detection remains the bigger challenge.

In your most recent external intrusion, did your organization determine how intruders gained access to your network?

- Yes: 58%
- No: 16%
- I don’t know: 26%

Similarly, it is encouraging to see that, nearly 60 percent of the time, organizations are able to determine exactly how intruders gained access to their networks. For the 42 percent who question their abilities, it is time to re-evaluate the tools and skills deployed to monitor and investigate network activity.

Has your audit or IT security department raised to senior management any concerns regarding the threat of network intrusion by unauthorized external parties?

- Yes: 73%
- No: 15%
- I don’t know: 12%
This is a question that would be interesting to track over time. Today, nearly three-quarters of respondents say that the topic of external intrusions has been raised to senior management. But would this have been the case five years ago? Perhaps not. But since the Target, Sony and OPM attacks, where senior leaders were held accountable for the breaches, these intrusions have clearly become a boardroom topic.

The next question reviews the business impact of external intrusions.

**What was the business impact of any intrusions?**

- Financial losses, including lost revenue, and/or incremental operational expenses: 20%
- Damage to the organization's reputation: 18%
- The intruders removed or deleted sensitive data: 10%
- I don't know: 3%
- None: 3%

Clearly, it's not just a matter that the technology failed. Breaches today are recognized for their tangible business impacts. And when assessing these impacts, respondents say that data compromise is the least of their three top concerns. The top two business impacts: Financial losses and reputational damage.

The next section looks at the impact of internal compromise.
III. Internal Abuse

For too many organizations, access is the gift that keeps on giving. Once an individual gains access to a critical system, that access is too rarely revoked – even when that individual moves on to a new role. In this section, respondents say:

- 91 percent are somewhat or very concerned about legitimate employees/contractors/vendors abusing their access privileges.
- 47 percent believe that former employees/contractors/vendors might be able to still change passwords on shared accounts.

What is your organization’s level of concern about legitimate employees, contractors or vendors abusing their privileged network access?

- Somewhat concerned: 55%
- Very concerned: 36%
- Not at all concerned: 9%

Never have we worked at a time when so many individuals had so much access to so much critical information. From onsite employees to remote contractors, vendors and partners, so many different individuals share privileged access to critical systems. And survey respondents are legitimately concerned about the risk of these individuals abusing their access in some way that compromises the organization.
Do you believe that former employees, contractors or vendors are familiar with your organization’s processes to change passwords on shared accounts?

- Yes, former employees, contractors or vendors would still recognize the password reset processes: 47%
- No, former employees, contractors or vendors were never privy to our processes: 28%
- I don’t know: 13%
- No, former employees, contractors or vendors would no longer recognize the processes we employ, as they have changed: 12%

Nearly half of the respondents say their former employees, contractors and vendors would still recognize how the organization changes passwords on shared accounts.

If this first line of network defense is so vulnerable, how about other existing processes? This question will be explored in the next section.
IV. Existing Processes

This section unveils several vulnerabilities that must be addressed by both policy and technology. Among the stand-out stats:

- Only 57 percent of respondents say their organizations have automated systems in place to deactivate access as people move out of the organization.
- 54 percent rate as average or below their users’ abilities to protect themselves from phishing and other social engineering attacks.

Does your organization have identity and automated access management in place to initiate and deactivate access as people move into and out of your organization?

Here, 57 percent of respondents say they do have automated systems in place to initiate and deactivate access as individuals transfer through the organization.

But that number is perhaps less significant than the 43 percent who do not yet have such tools in place.

**Does your organization have password management automation to enforce password strength policies and enable users to reset forgotten passwords or clear lockouts?**

Nearly three-quarters of respondents have deployed some form of password management automation to enforce policies and help users either reset forgotten passwords or clear lockouts.

But that’s only one layer of defense. Moving on ...

Frequently, we hear about “access creep,” where individuals never relinquish any of the system access they gain in an organization – even when they move into new roles that no longer require the old access.
Do you believe the process used by your organization’s help desk to authenticate callers is secure enough to prevent an attacker from overcoming it via spoofing?

54%  Yes, I believe the process is secure and prevents spoofing
29  No, I believe the process is insecure and unable to prevent spoofing
 9  I don’t know
8  We do not have a formal help desk

The help desk shows a weak underbelly for organizations. Only 54 percent of respondents say their help desks have a secure process to authenticate callers and prevent “spoofing” attacks. The remaining 46 percent are vulnerable to social engineering attackers who know how to worm their way into privileged accounts, where their activity may go undetected.

How do you assess your organization’s users’ ability to protect against phishing and similar social engineering attacks?

45%  Average
40  Above Average
8  Below Average
6  Superior
1  Failing

And, indeed, when it comes to social engineering attacks via phishing and other techniques, only 46 percent of respondents say their users have above average or superior defensive capabilities.

This remains one of the key soft spots in any secure organization. No matter the policies or tools deployed, security is only as strong as the decisions people make when confronted by the trickery of social engineers.

Does your organization have processes in place to change passwords on shared or privileged accounts?

75%  Yes
18  No
7  Not currently, but we plan to deploy such a system

Recognizing the potential risks of passwords on shared or privileged accounts, 75 percent of respondents say their organizations do have processes in place to change these passwords, a fundamental element of defense.

Next, respondents share some of the specific security controls they have deployed.
V. Infrastructure

When reviewing specific security controls that have been deployed, it is somewhat surprising to find:

- Only 52 percent of organizations have deployed multifactor authentication to high-risk or highly-privileged users
- Only 40 percent have deployed automation to control access to shared accounts

Read on to learn more about current controls.

Has your organization deployed a multifactor authentication technology for your high-risk or highly privileged users?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Not currently, but we plan to deploy such a system</th>
</tr>
</thead>
<tbody>
<tr>
<td>42%</td>
<td>40</td>
<td>19</td>
</tr>
</tbody>
</table>

It is a significant red flag that not even half of responding organizations have deployed multifactor authentication to their high-risk or highly privileged users. This is the equivalent of installing a sophisticated home security system ... but neglecting to lock the front door.

If you answered yes to the previous question, which of the following multifactor authentication technologies has your organization deployed?

- RSA SecurID or similar token: 61%
- App on smart phone: 27%
- Soft token: 27%
- PIN sent to user’s phone: 23%
- Smart Card: 23%

For those organizations that have deployed MFA, the most common element are the classic RSA SecurID (or similar) tokens, soft tokens and apps on smart phones. Smart cards and PINs sent to users’ phones also are common to nearly one-fourth of organizations.
If your organization has not deployed multifactor authentication technology, what are the reasons?

We plan to deploy in the future: 39%
We have inadequate management support: 30%
We do not possess the budget: 29%
In order to deploy MFA, we must overcome interoperability problems: 14%

For those organizations that do not deploy MFA, nearly 40 percent say they plan to do so in the future. But 30 percent of respondents say they do not have management support for MFA deployment, and 29 percent say they lack the budget.

Clearly, this emerges as one strong element around which to build a business case for deployment.

21. Has your organization deployed automation to control access to shared, privileged accounts?

Yes: 40%
No: 42%
Not currently, but we plan to deploy such a system: 18%

In terms of automation, only 40 percent of organizations say they have deployed automated tools to control access to shared, privileged accounts. This means that 60 percent are entrusting access to monitoring by people – or they are not paying attention at all to this vulnerable vector. This is a door that organizations do not want to leave ajar, given the concerns they have expressed about the potential for internal abuse.

What percentage of your organization’s systems and applications do you believe are in-scope for automated access control today?

Under 10%: 12%
10%-25%: 14%
26%-50%: 15%
51%-75%: 24%
76%-100%: 22%
None: 13%

One-quarter of respondents say their organizations have between 50 and 75 percent of their systems and applications in-scope for automated access control today. That’s the baseline from which organizations must build their 2016 business plans and budgets to automate access to the remaining systems and applications.

Next, the report will review how budget is allotted – and what to expect for funding in 2016.
VI. The Cost of Security

We know security is an enterprise priority, but how much attention is being paid to privileged access management? Here we learn:

- 29 percent of respondents say their current security budgets represent 1-10 percent of the IT budget
- 40 percent say of that security budget, 1-10 percent is assigned to strong authentication

Here is a review of current funding trends:

What proportion of your IT budget is currently assigned to information security?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Number of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>I don't know</td>
<td>35%</td>
</tr>
<tr>
<td>1-10%</td>
<td>29</td>
</tr>
<tr>
<td>11-20%</td>
<td>15</td>
</tr>
<tr>
<td>21-30%</td>
<td>10</td>
</tr>
<tr>
<td>41-50%</td>
<td>4</td>
</tr>
<tr>
<td>31-40%</td>
<td>4</td>
</tr>
<tr>
<td>50%+</td>
<td>3</td>
</tr>
</tbody>
</table>

From that security budget, 40 percent say 1-10 percent is dedicated to strong authentication. Another 15 percent say 11 to 30 percent could be allocated.

Start with the IT security budget, which typically is a portion of the overall IT budget. Nearly one-third of respondents say security is 1-10 percent of the IT spend. Twenty-five percent say that security budget can range from 11 to 30 percent.

What proportion of the security budget is assigned to strong authentication?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Number of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>I don't know</td>
<td>41%</td>
</tr>
<tr>
<td>1-10%</td>
<td>40</td>
</tr>
<tr>
<td>11-20%</td>
<td>9</td>
</tr>
<tr>
<td>21-30%</td>
<td>6</td>
</tr>
<tr>
<td>41-50%</td>
<td>2</td>
</tr>
<tr>
<td>31-40%</td>
<td>1</td>
</tr>
<tr>
<td>50%+</td>
<td>1</td>
</tr>
</tbody>
</table>
When focused specifically on privileged access management, 41 percent of respondents say 1-10 percent of the security budget may be allocated here.

And then, when focused specifically on privileged access management, 41 percent of respondents say 1-10 percent of the security budget may be allocated here. Thirteen percent say that range is from 11 to 30 percent.

With those figures in mind, look next at projected spending plans for 2016.
There is encouraging news for the coming year:

- 32 percent of respondents expect increases in their budgets dedicated to privileged access management
- Multifactor authentication is one of the top three technology tools planned for deployment

What else is on the 2016 agenda?

In the next 12 months, how will your organization’s security budget dedicated to privileged access management change?

- 43% I don't know
- 26% It will not change
- 18% It will increase 1-5%
- 8% It will increase 6-10%
- 5% It will increase more than 10%

No organization articulates a planned decrease in budget dedicated to privileged access management. That's encouraging news. Better yet: 57 percent expect this funding to either stay the same or to increase anywhere from 1 to more than 10 percent.
Respondents have broad plans to improve privileged access management across the board in the year ahead. The top three planned investments are: Audit tools, multifactor authentication and intrusion detection. But next on the list: password management and a privileged access management system.

Given all these statistics, what messages can we draw from the survey — and how can organizations put these results to work to improve privileged access management?

In the closing sections of this report, key conclusions will be offered, and then Idan Shoham of survey sponsor Hitachi ID Systems will offer color commentary on what these conclusions mean, and how to incorporate them in your 2016 security strategy.
Conclusions

A thorough review of the survey results brings us to these summary conclusions:

Recognize the Risks
Target, OPM, the NSA – pick a high-profile data breach, and chances are it resulted from identities or access compromised by an intruder who was given or who stole privileged access to a critical network or system. Behind every large breach, it seems, there is a simple, preventable access point. The risks are real, the consequences are costly, and the argument is rock solid: It’s time to improve how enterprises manage identities and privileged access.

Raise the Baseline
When it comes to breach prevention, “average” is nowhere near good enough. “Average” is why so many targeted organizations have been breached – because they have not rolled out controls such as multifactor authentication and automation for passwords and access management. To avoid being the next headline, organizations must raise this security baseline.

Multifactor Authentication is the New Standard
Although government regulators and standards bodies have long called for a minimum of two-factor authentication for critical networks and systems, too few organizations have actually moved beyond simple passwords and data that can be purloined by keyloggers. It’s time to heed the warnings and respond to the string of recent attacks. Passwords are not dead – but they must be given new life by being used in conjunction with tokens, pins, biometrics and other robust authentication technologies. To not embrace multifactor authentication is to be negligent.

Privileged Access Management is a Not a Deployment
This survey reveals multiple pain points. Organizations are vulnerable to external attackers and to trusted insiders, and they have done little to protect mission-critical networks and systems beyond user name and password. Processes are not being followed, the right authentication tools have not been deployed, and security staff is not trained sufficiently to manage the tools that are in place. The business case has been made for privileged access management, but it is important not to approach that as a discrete project – it’s a program. It involves tools, training and ongoing monitoring to ensure that organizations can manage privileged identities with automation, and that they can improve their abilities to prevent external/external intrusions before critical data is altered, deleted or stolen.

In the closing section of the report, Idan Shoham of Hitachi ID Systems will discuss privileged access management and how one can use the results of this survey to make the business case for such a program.
How to Maximize Your Privileged Access Management Program

Survey Analysis by Idan Shoham, CTO of Hitachi ID Systems

Note: In preparation of this report, ISMG VP Tom Field sat down with Hitachi ID Systems CTO Idan Shoham to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

In his role as Chief Technology Officer, Shoham is responsible for defining product and technology strategy and the overall development of Hitachi ID Systems solutions. He works closely with his talented team to ensure that the solutions that Hitachi ID Systems delivers to the market are of the highest quality. Prior to founding Hitachi ID Systems in 1992, Shoham provided network security consulting services to large organizations such as Shell, Amoco, BP Canada and Talisman Energy. He holds a Masters degree in Electrical and Computer Engineering.

‘We Can Do Better’

TOM FIELD: Okay, Idan, we’ve had a chance to go through the survey results. What’s your gut reaction? What are the key points that strike you and maybe even surprise you?

IDAN SHOHAM: The first thing that strikes me is that IT security budgets are relatively small, and that goes a long way to explaining the string of public exploits that you’ve read about in the press over the past few years. The second thing that’s interesting here is: People’s self-assessment is generally positive, but then if you look at the assessment of their risks, they’re pretty elevated. I think people are basically saying, “We’re doing pretty well compared to our peers, but we have serious issues,” which implies that everybody’s got serious issues around strong authentication, around deactivating access, around automation. As an industry, I think we can clearly do better.

Overconfident About Access Management

FIELD: Idan, it strikes me that the respondents seemed a little bit overconfident on the surface at least about their abilities to manage privileged identity and access. Do you agree? And if so, in your experience, where does that overconfidence come from?

SHOHAM: I think people look at their own organizations, and then they talk to peers to get a sense of where they stand vis-à-vis the other organizations, and in that sense you would expect most people see themselves as average: that’s what average means. I think that there’s a dichotomy between people’s view of their organization vis-à-vis other organizations versus their view of how they’re doing vis-à-vis absolute risk. People are saying, “Yes, we’re doing about the same as everybody else,” which is not surprising, and at the same time they’re saying, “and we have these substantial risks,” which is also true. I don’t think that these two things are in any way mutually exclusive. They’re just two ways to look at an organization’s security posture, and I think my advice would be focus on actual risk; don’t focus on what your peers are doing. If your organization gets hacked
and you turn up on the front page of the local newspaper, that’s a concrete consequence, and the fact that your peers who have similar controls didn’t happen to get hacked in the same way, that’s not much comfort. The focus needs to be on absolute risk, and I think people have a fairly good assessment of what their risk profile actually is.

The Detection Deficit

FIELD: We talked about external intrusions in the survey, and when you look at the results, detection seems to be the major hurdle for organizations. When it comes to detection, what are organizations typically overlooking?

SHOHAM: I don’t know that they’re overlooking anything. I think in order to detect active or attempted intrusions and attacks, you need a pretty sophisticated infrastructure. You need sensors on your network; you may need sensors on the endpoints. You need log and data aggregation, you need pattern matching analytics. You need the dashboards - this is a lot of technology. I would expect medium-to-large enterprises to have this kind of sophisticated surveillance. Larger organizations typically have a security operations center of some sort. I know that small organizations generally don’t, and they probably can’t afford it. The advice here is, if you’re too small to afford building your own sensor networks and surveillance and so forth, farm this function out. There are a number of companies out there that operate managed security services, and smaller organizations can leverage these services relatively inexpensively. These providers keep an eye on your network for you. Even quite small organizations, if they have something worth protecting, need this kind of surveillance.

Internal Access Risks

FIELD: Switching the conversation to internal access, we see that respondents are concerned about current and former employees, contractors, vendors, how they behave. We always hear about access creep and privileges that never go away. How do we put this animal back in the cage?
SHOHAM: There’s decent technology for that. Here at Hitachi ID, we’re in the business of making software to address this problem. There are really two styles of access. There are business user accounts -- e-mail accounts, CRM accounts and so forth. These are basically end-user access rights, and organizations manage these through automation, through roles, through policies, through periodic access certification and so forth. There are quite mature products to manage these kinds of access rights. Traditionally the cost of these systems has been mainly consulting fees to deploy them, but that’s coming down as vendors like us bring to market implementations that are less expensive to set up.

The other pattern is privileged access. These are typically shared, high privilege IDs, for example root on Linux and Administrator on Windows. The way these are managed is different, because the accounts often already exist when a system is deployed and remain even as their human owners turn over. Without automation, you typically have static, well-known passwords - often stored as plaintext and shared by many people. That’s obviously a security issue, especially as people move into and out of the organization.

There is a whole other category of software to secure these accounts: privileged access management products, of which we make one. The idea is to set the passwords on these accounts to random, frequently changing strings and then to launch login sessions, without necessarily displaying passwords, for authorized users. This way, access is granted for short periods of time -- for hours, not days or weeks.

Twenty years ago there were no products to do this. Ten years ago, there was really early code. Today, there are quite sophisticated and mature products in this space, and I think the consulting effort required to deploy them and the amount of automation that they bring to bear to reach into the environment and discover and integrate systems is quite mature. What that means in practice is that the TCO, the barrier to entry, is coming down, and smaller organizations can cost-justify automating privileged access management.

“If you’re too small to afford building your own sensor networks and surveillance and so forth, farm it out.”
“The barrier to entry is coming down, and smaller and smaller organizations can cost-justify automating privileged access management.”

FIELD: Clearly, the technology has evolved. Do you see people and processes evolving as well to leverage those technologies, or do you still have a cultural gap you have to get over in many organizations?

SHOHAM: I think the processes are definitely evolving. I’ll give you concrete example. One way that organizations that didn’t have good technology to control access to privileged accounts was cut passwords in half - the first five characters and the last five characters, for example - and give those halves to different people. If you wanted to log into a really high privileged account, both of those people would have to get together at the keyboard, and one would type five characters, and then the other would type the rest. That’s really low tech, and today there’s absolutely no reason to do that, where you have password randomization, vaulting, workflow, single sign-on and screen recording.

What’s changed? When we would have conversations with organizations as recently as two years ago, we were still getting requests to automate this low tech, password slicing strategy. We would say, “Sure, we could do that for you, but there are better ways to address this control problem.” I don’t recall in the last year or two having anyone us to do that, so there’s definitely a gradual transition away from low-tech to more sophisticated controls.

Must-Have Tools

FIELD: As you look to 2016, what do you see as the must-have tools to enable a robust privileged access management program?

SHOHAM: I think you need a few things. First of all, you need management mandates to do this! You’re not going to get anywhere if you don’t have the organizational support to do it, and frankly, funding to implement stronger controls. Beyond that, you need technology. Privileged access management done manually is an incredible pain. You need to purchase products that can discover systems in the infrastructure, classify them, apply policy to them, randomize passwords, control access to privileged accounts, record sessions and so forth. We make software in this space, as do others. It’s a mature, robust, lively marketplace where you can buy quite advanced capabilities.

The other thing that you really need is two-factor authentication. It seems to me strange that you’d go to all this trouble to secure privileged accounts, and then all these privileged accounts are accessible behind a sort of firewall of an authentication step, and that firewall ought not to be yet another password, and a static one at that. That just seems like reverting to the problem that you’re trying to solve. At least the process that you use to sign into a privileged access management system ought to be a multifactor authentication, and it doesn’t have to be expensive. It can be as simple as when you log in, the system sends a PIN to your phone or to your personal e-mail, and then you have to enter that before you enter your password. Fundamentally, it has to be something that isn’t vulnerable to a keylogger, because there’s malware out there, and people’s endpoints, their laptops, their PCs, sooner or later get compromised. If your PC is compromised, some attacker in some other country will deploy a keylogger on your PC, will steal your password and will be able to sign into anything as you - and that includes into the privileged access management system. The keylogger has got you, so you need something that a keylogger can’t replay, and that’s really what we mean by 2FA, or two factor authentication.

Making the Case for PAM

FIELD: How do you recommend that security leaders build that business case for management to support that program and invest in it, and what would you say might be the key ROI factors that could get management’s attention once you deploy and start to measure results?

SHOHAM: Let me start with the second part first. I don’t think that ROI is really the right way to think about it. It’s really risk mitigation that we’re talking about, so you’re talking about risks of massive compromise of private data or of corporate IP or rogue trading or safety problems or penalties triggered by regulatory compliance problems. We’re talking about catastrophic failures in your internal controls and how to avoid them. When people talk about “regulatory compliance” this is really what they really mean: “how to comply with regulations that mandate strong enough internal controls, designed to minimize the risk of catastrophic failures.” That’s really what’s underlying this, and I think you have to present your business case to management in those terms.
You have to start by saying: “There’s this hypothetical catastrophic failure that I’m worried about, and if this happens -- and the probability is not high -- let’s not pretend that this is absolutely going to happen in the next three years; the probability is relatively low for any given kind of incident to happen in any given organization, but the consequences of failure are substantial.” In the UK recently, TalkTalk was hacked, and millions of customer records were leaked -- exfiltrated. Will that company survive the experience? I don’t know. In the US, Target got hacked. Their point of sale systems were all compromised. The impact on the valuation of the company was in the billions of dollars, so the consequences are extreme for these incidents, and really you’re talking about reducing the risk of an extreme negative outcome from maybe single digits to less than 1 percent. I think that’s how you pitch it to the organization.

How do you pitch PAM as opposed to other security tools? I think you have to lay out the scenario that you want to defend against. One scenario that PAM systems mitigate is insiders who become malicious. This happened to the city of San Francisco a few years ago, where a network admin set all the credentials on all the network routers, basically locking everyone else out of network management. That admin held the city of San Francisco, the entire municipal government hostage. The other kind of incident is an attacker who has physical access to your network perimeter, or somebody who compromises one of your PCs with malware -- basically an outsider with a beachhead in the environment, and they expand their reach from that starting point. Both of these are problems that can be reduced with a privileged access management system, because you take away the ability of a keylogger to propagate the connection from one system to another. You introduce 2FA into all your sessions, and you change static passwords, so if a password is compromised, the period of time that it’s good is very short, and you get away from the same password being used on many systems. If one password is compromised, only that system is compromised. Basically, you’re creating barriers inside your perimeter, so that a small compromise does not quickly become a large compromise, and you’re creating forensic audit trails. I think that’s essentially how you pitch the solution: as a way to slow down the expansion of a successful initial penetration and as a way to create forensic audit, which are helpful both against malicious insiders and successful outsiders. You talk to your management about the risk of catastrophic control failures, and then you draw them a picture of how an attacker might actually progress through the environment to go from initial ingress to catastrophic access, and then you show them how this kind of system would prevent this escalation.

“How much risk can you tolerate and how much money are you willing to spend as an organization to mitigate [risk]?”

Put the Survey to Work

FIELD: How do you recommend the security leaders use our survey results and put them to work?

SHOHAM: Ask for money.

It sounds cheesy, but it’s true. IT security is a small percentage of IT spends, and I think it ought to be a somewhat larger proportion of IT spending, and that’s not just for procuring technology like our products -- it’s also to grow your organization. I think you need an IT security program, you need a privileged access management program, you need multifactor authentication to play a part in that. You need one or two people who are technically very smart to help you implement these systems and to maintain them, keep them operating, and to expand their scope over time. Both people and technology cost money, and I think a survey like this helps IT security leaders build a narrative for their management, explaining what the risks are and how those risks might materialize in practice and what kind of investment they require to mitigate the risks.

I think if you do a good enough job explaining the risks and the probabilities of compromise both before and after deploying these systems, then it becomes a business decision, and I think that’s what it ought to be -- not about whether to implement some security software, but how much risk can the organization tolerate and how much money is the organization willing to spend to mitigate the risk?

For more results and analysis from the 2015 Privileged Access Management Study, please see: http://hitachi-id.com/cgi-bin/emaildoc?document=Web873-HitachiID.pptx
Want to learn more about privileged access management?
Check out these content resources.

Path to Privileged Access Management
Hitachi ID Systems’ Shoham on the Business Drivers, Benefits

Wary of intrusions, data compromise and theft, organizations increasingly are deploying privileged access management solutions. Idan Shoham of Hitachi ID Systems offers the essential do’s and don’ts.

Breach prevention is one of the key business drivers, says Shoham, CTO and founder of Hitachi ID Systems. But there also is concern to avoid regulatory penalties or negative publicity that could result from the wrong person accessing privileged data.

“At the end of the day, these are all dimensions of security,” Shoham says. “People are basically worried about securing their infrastructure and their data.”

And fair warning, he adds: The biggest deployment challenges are not technical; they’re organizational.

In an interview about privileged access management, Shoham discusses:

- The business drivers for privileged access management;
- The essential do’s and don’ts;
- How to prioritize a PAM deployment.

http://www.inforisktoday.com/interviews/path-to-privileged-access-management-i-2753

RESULTS WEBINAR

2015 Privileged Access Management Study:
The Results

Presented by Idan Shoham and Tom Field

Whether seeking to block external attacks or curb internal abuse, security-conscious organizations increasingly are focusing their efforts on protecting the true crown jewels: privileged identities.

Do you have confidence in your organization’s ability to manage privileged identities and prevent their abuse? Can your security team detect and identify intruders before data disappears? Are you confident that former employees and contractors no longer have access to your critical systems?

Register for this session to see results of the 2015 Privileged Access Management Study and learn:

- How organizations can best managing privileged identities;
- The true business impact of intrusions due to external/internal privileged users;
- Modern methods being employed to detect both accidental and malicious activity.

Idan Shoham of Hitachi ID Systems will provide exclusive survey analysis and insight on how to employ these survey results to improve how your organization manages and secures privileged identities and access.

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG’s subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
sales@ismgcorp.com