RETHINKING IAM: HOW A RISK-BASED, AUTOMATED APPROACH MAKES IDENTITY AND ACCESS MANAGEMENT MORE STRATEGIC AND EFFECTIVE

Frank Bresz
Executive Director, Advisory Services Cybersecurity
Ernst & Young LLP
@frankbresz

Stephen Mowll
Director, Product Management Lead – RSA Identity G&L
RSA
@Smowll

#RSACharge
METHODOLOGY & OBJECTIVES

Sample

<table>
<thead>
<tr>
<th>Field Work</th>
<th>This survey was fielded in January 2016.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Respondents</td>
<td>104 qualified completes</td>
</tr>
</tbody>
</table>

Method

<table>
<thead>
<tr>
<th>Collection</th>
<th>Online Questionnaire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Questions</td>
<td>11 (excluding screeners and demographics)</td>
</tr>
<tr>
<td>Audience</td>
<td>To qualify for this survey respondents were required to work for an organization with 500+ employees at Director level or above in an IT security, risk management, and/or compliance-related job function.</td>
</tr>
</tbody>
</table>

Survey Goals

The purpose of this survey was to understand usage and perceptions of identity and access management (IAM). In addition to evaluating IAM deployment, we also determined the current and ideal level of automation for IAM, and discovered whether organizations assess the risk levels of enterprise applications, how risk data is leveraged, and the benefits associated with the use of application risk data to automate IAM-related controls.

Source

IDG Research surveyed 104 IT decision makers in December 2016 and January 2017 on behalf of Ernst & Young, LLP and RSA Security LLC, a subsidiary of Dell EMC Infrastructure Solutions Group, to support this survey and its results.
## Respondent Profile

### Organization Size

<table>
<thead>
<tr>
<th>Size Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>100,000 or more</td>
<td>10%</td>
</tr>
<tr>
<td>50,000 - 99,999</td>
<td>11%</td>
</tr>
<tr>
<td>30,000 - 49,999</td>
<td>3%</td>
</tr>
<tr>
<td>20,000 - 29,999</td>
<td>6%</td>
</tr>
<tr>
<td>10,000 - 19,999</td>
<td>11%</td>
</tr>
<tr>
<td>7,500 - 9,999</td>
<td>4%</td>
</tr>
<tr>
<td>5,000 - 7,499</td>
<td>6%</td>
</tr>
<tr>
<td>2,500 - 4,999</td>
<td>15%</td>
</tr>
<tr>
<td>1,000 - 2,499</td>
<td>22%</td>
</tr>
<tr>
<td>500 - 999</td>
<td>13%</td>
</tr>
</tbody>
</table>

**Mean number of employees:** 23,492

**Median number of employees:** 3,750

### Job Title

<table>
<thead>
<tr>
<th>Title</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSO (Chief Security Officer)</td>
<td>8%</td>
</tr>
<tr>
<td>CISO (Chief Information Security Officer)</td>
<td>16%</td>
</tr>
<tr>
<td>CRO (Chief Risk Officer)</td>
<td>4%</td>
</tr>
<tr>
<td>CCO (Chief Compliance Officer)</td>
<td>4%</td>
</tr>
<tr>
<td>CIO (Chief Information Officer)</td>
<td>13%</td>
</tr>
<tr>
<td>CTO (Chief Technology Officer)</td>
<td>13%</td>
</tr>
<tr>
<td>CEO, President, Owner, Partner</td>
<td>5%</td>
</tr>
<tr>
<td>COO, General Manager, Executive Director, Managing Director</td>
<td>1%</td>
</tr>
<tr>
<td>Executive Vice President, Senior Vice President, Vice President</td>
<td>10%</td>
</tr>
<tr>
<td>Director</td>
<td>27%</td>
</tr>
</tbody>
</table>

### Job Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology (IT) Security (including identity and access management)</td>
<td>91%</td>
</tr>
<tr>
<td>Risk Management or Risk Governance</td>
<td>57%</td>
</tr>
<tr>
<td>Compliance or Audit</td>
<td>46%</td>
</tr>
</tbody>
</table>

### Top Represented Industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health care (providers and pharmaceutical)</td>
<td>19%</td>
</tr>
<tr>
<td>Financial services (banking, insurance, brokerage)</td>
<td>15%</td>
</tr>
<tr>
<td>Government or Nonprofit (including education)</td>
<td>15%</td>
</tr>
<tr>
<td>High tech</td>
<td>13%</td>
</tr>
<tr>
<td>Retail, wholesale and distribution</td>
<td>9%</td>
</tr>
</tbody>
</table>
KEY FINDINGS

CURRENT IAM LANDSCAPE

- Organizations are more inclined to view IAM as a way to enable strategic objectives versus simply a business requirement. This is especially true of those whose primary function is IT security.

- More than 40% use multiple solutions to manage user IAM.
  - More than half of those using several different solutions find this to be highly challenging (51% extremely/very challenging).

- Organizations would prefer to see an increase in the level of automation applied to IAM.
  - Those primarily in compliance or audit roles are the most likely to be in favor of complete automation.

APPLICATION RISK DATA

- The majority of organizations (91%) are assessing the risk level of at least some enterprise apps. They primarily evaluate compliance (72%), data location (67%), and threat information (67%) to determine risk level.

- Exactly half of organizations are leveraging app risk data to automate IAM-related controls.

- Almost 6 in 10 respondents (58%) see leveraging application risk data to automate IAM-related controls as extremely/very valuable. A variety of benefits are associated.
SURVEY RESULTS
CURRENT IAM LANDSCAPE
Organizations are more inclined to view IAM as a way to enable strategic objectives rather than a business requirement.

Q1: What is the status of user identity and access management (IAM) at your company (e.g., management of user profiles, authentication, authorization and access privileges across system and enterprise boundaries)?

Base: 104 qualified respondents

Status of IAM

1: IAM is required to maintain security and compliance.

Mean: 6.5

Median: 7

10: IAM is a business service enabling strategic objectives.

Those whose jobs primarily focus on IT security are five times as likely to view IAM as a strategic investment versus those in risk management or compliance roles.

Q1: What is the status of user identity and access management (IAM) at your company (e.g., management of user profiles, authentication, authorization and access privileges across system and enterprise boundaries)?

Base: 104 qualified respondents
MORE THAN 40% USE MULTIPLE SOLUTIONS TO MANAGE USER IAM. OVER HALF OF THOSE USING SEVERAL DIFFERENT SOLUTIONS FIND THIS TO BE HIGHLY CHALLENGING.

**Management of User IAM**

- Centrally managed with a single solution
- No IAM solution in place, but currently evaluating solutions
- Not centrally managed (using several different tools or solutions)
- No IAM solution in place and no plans to evaluate solutions

### Centrally managed (43%)

- 14% No IAM solution in place, but currently evaluating solutions
- 37% Not centrally managed (using several different tools or solutions)
- 37% No IAM solution in place and no plans to evaluate solutions

### Multiple solutions (41%)

- 11% No IAM solution in place, but currently evaluating solutions
- 5% Not centrally managed (using several different tools or solutions)
- 12% No IAM solution in place and no plans to evaluate solutions

**Those more likely to indicate user IAM is centrally managed:**

- Report IAM is highly automated
- Tend to be smaller enterprises

**Challenge to Integrate Multiple User IAM Tools**

(out of those without centrally managed IAM tools)

- 14% Extremely challenging
- 37% Very challenging
- 37% Somewhat challenging
- 12% Not very challenging

**Q2: How is your company handling user IAM today?**

Base: 104 qualified respondents

**Q3: How challenging is it for your organization to integrate and coordinate multiple user IAM tools?**

Base: those without centrally managed IAM tools: 43 qualified respondents
ORGANIZATIONS WOULD PREFER TO SEE AN INCREASE IN THE LEVEL OF AUTOMATION APPLIED TO IAM.

Level of Automation in IAM Approach Today

- 23% Completely manual
- 33% Mostly manual, some automated processes
- 25% Even mix of manual and automated processes
- 11% Mostly automated, some manual processes
- 8% Completely automated
- 2% Don’t know

Ideal Level of Automation in IAM Approach

- 35% Completely manual
- 16% Mostly manual, some automated processes
- 41% Even mix of manual and automated processes
- 6% Mostly automated, some manual processes
- 2% Don’t know

Those primarily in compliance or audit roles are the most likely to be in favor of complete automation.

Q4a: How would you describe the level of automation around your company’s approach to IAM today?
Q4b: What level of automation around IAM would be ideal for your company?
Base: 104 qualified respondents
LEVERAGING APPLICATION RISK DATA
Assessing Risk Level of Enterprise Apps

- Yes, for all applications: 38%
- Yes, for some applications: 8%
- No, not at all: 53%
- Don’t know: 2%

Criteria When Determining Risk Level

- Compliance requirements or audit information: 72%
- Location information (e.g., cloud, on premises): 67%
- Threat information: 67%
- Incident data: 57%
- Behavior analytics: 38%
- Device fingerprint (device types that access the application): 27%
- Other: 5%
- Not applicable: 2%

Q5: Does your organization assess the risk level of enterprise applications (e.g., low, medium, high, critical)?
Q6: When determining the risk level of an enterprise application, which of the following does your company consider?

Base: 104 qualified respondents

Those who have mostly/completely automated IAM consider this an important criteria.
Exactly half of organizations surveyed are leveraging app risk data to automate IAM-related controls.

### Leveraging App Risk Data to Automate IAM-Related Controls

- **Yes**: 50%
- **No**: 39%
- **Don’t know**: 11%

### How Companies are Leveraging App Risk Data (of those leveraging app risk data)

- Leveraging approval workflows based upon risk: 63%
- Executing and managing access certifications based upon risk categorization of applications: 58%
- Performing step-up authentication based upon an application’s risk rating: 42%
- Other: 4%

Q5: Does your organization assess the risk level of enterprise applications (e.g., low, medium, high, critical)?

Q6: When determining the risk level of an enterprise application, which of the following does your company consider?

Base: 104 qualified respondents
Almost 6 in 10 decision-makers see leveraging application risk data to automate IAM-related controls as extremely/very valuable.

Value in Leveraging App Risk Data to Automate IAM-Related Controls

- Extremely valuable: 6%
- Very valuable: 16%
- Somewhat valuable: 36%
- Not very valuable: 42%

Benefits Associated with Use of App Risk Data to Automate IAM Controls

- Increased automation reduces time spent by IT staff modifying access controls: 39%
- More proactive approach to access management: 38%
- Improved compliance management: 38%
- Higher assurance authentication: 31%
- Simpler integration of new technology services (e.g., cloud applications): 30%
- Ability to implement incident response plans more rapidly: 26%
- Business or user friendly (avoid over-complication of security around low-risk applications): 24%
- Increased autonomy of business mgrs to grant users access to enterprise info without IT’s involvement: 22%
- Simplified or more streamlined IAM processes: 21%
- None: 2%

Q9: How valuable is it or would it be to leverage application risk data to orchestrate and automate IAM-related controls?

Q10: What are the top benefits you associate with the use of application risk data to orchestrate and automate IAM-related controls?

Base: 104 qualified respondents

Those still evaluating IAM solutions see this as the top benefit.
Frank Bresz
Executive Director
Advisory Services
Cybersecurity
Ernst & Young LLP
@frankbresz
+1 212 773 3788
frank.bresz@ey.com

Follow us on twitter:
@EY_Alliances

Find us on:
ey.com/alliances

Engage with us:
bit.ly/EY_Alliances

RSA Archer Governance, Risk and Compliance Group
bit.ly/2y6ZfPk
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY’s Advisory Services
EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

The better the question. The better the answer. The better the world works.

© 2017 Ernst & Young LLP.
All Rights Reserved.

SCORE No.
1709-2412815

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com