Only 34 percent of surveyed security leaders say they have high confidence in their organization’s ability to detect and prevent fraud before it results in serious business impact. Among the reasons why they lack confidence:

- Today’s fraud schemes are too sophisticated and evolve too quickly (56 percent of respondents)
- Customers and/or partners lack sufficient awareness to protect themselves from socially-engineered schemes (56 percent)
- Employees lack that same awareness (52 percent)

These are among the results of the 2016 Faces of Fraud Survey, sponsored by SAS and focused on The Analytics Approach to Fraud Prevention.

ISMG has conducted this survey for seven years now, but this is the first time under SAS sponsorship and with a focus on – as the title says – the Analytics Approach to Fraud Prevention.

Encouraging news from the survey results? Forty-six percent of respondents say they actively deploy advanced data analytics to monitor transaction/program activity and predict the likelihood of fraud.

But there is also concerning news: Forty-two percent say they lack the staff expertise to successfully deploy advanced data analytics tools, and 45 percent say their current systems allow for only limited analytics.

Read on for a detailed look at the forms of fraud afflicting financial and government organizations; their current security controls – and gaps; and where they plan their biggest anti-fraud investments for 2017.

Best,

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com
This anonymous survey was conducted online by the ISMG research team during the spring of 2016, targeting C-level security and technology leaders at financial and government organizations. The survey attracted more than 240 respondents from organizations across global regions, with emphasis on the U.S.

Introduction ............................................................................... 2

By the Numbers ......................................................................... 4

Survey Results
Baseline Fraud Defense ............................................................. 5
2016 Faces of Fraud ................................................................. 8
Enterprise Fraud Prevention ..................................................... 16
2016 Fraud Agenda ................................................................. 21

Conclusions ............................................................................. 23

Survey Analysis
David Stewart, Shaun Barry and Ian Holmes of SAS .............. 24

About the Sponsor:

SAS is the leader in analytics. Through innovative analytics, business intelligence and data management software and services, SAS helps customers at more than 80,000 sites make better decisions faster. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®.
By the Numbers

Some statistics that jump out from this study:

67%
67 percent of respondents say it takes one day or more to uncover a fraud incident once it occurs.

56%
56 percent say customers and/or partners lack sufficient awareness to protect themselves from socially engineered schemes.

54%
54 percent are not currently deploying advanced data analytics tools.
Baseline Fraud Defense

On one hand, survey respondents have moderate to high confidence in their organizations’ abilities to detect and respond to fraud when it occurs.

And yet …

More than half also say that today’s fraud schemes are too sophisticated and quick-changing to keep pace, and their own customers, employees and partners lack the fraud awareness to avoid falling victim to predatory scams.

This conflict captures perfectly the message of this opening section of the report. Full results follow.

What is your level of confidence in your organization’s ability to detect and prevent fraud before it results in serious business impact on your enterprise or your customers?

- High confidence - we have top-notch anti-fraud tools and professionals fighting fraud
- Moderate confidence - despite our best efforts, we occasionally miss a fraud scheme
- Low confidence - our anti-fraud tools and team just cannot keep pace with evolving fraud schemes
- No confidence - our customers are more apt to discover a fraud scheme before we do

On the surface, when asked a general “how do you feel …?” question, respondents from financial and government entities are quite positive about their confidence in their organizations’ abilities to detect and prevent fraud. An overwhelming 84 percent express either moderate or high confidence.

Sentiments change, however, when one digs deeper and probes about specific vulnerabilities. At that point the outer shell cracks a little. See below …

More than half also say that today’s fraud schemes are too sophisticated and quick-changing to keep pace, and their own customers, employees and partners lack the fraud awareness to avoid falling victim to predatory scams.
Survey Results

What do you believe to be the top three vulnerabilities in your fraud defenses? (select three that apply)

- Today's fraud schemes are too sophisticated and evolve too quickly for us to keep pace (56%)
- Our customers and/or partners lack sufficient awareness to protect themselves from socially engineered fraud schemes (56%)
- Our employees lack sufficient awareness to protect themselves from socially engineered fraud schemes (52%)
- We lack the technology tools to properly detect and respond to fraud (32%)
- We lack the in-house expertise to properly detect and respond to fraud (32%)

It has become cliche to refer to today's schemes as “sophisticated” or “evolving.” Yet, that is precisely what they are, and because of that, organizations struggle to keep their defenses on par.

Further, respondents acknowledge that their customers, partners and employees lack the awareness to protect themselves from socially engineered fraud schemes – many of which today are launched without even a malware component.

To what degree does your organization currently use advanced data analytics tools (i.e. behavioral analytics, predictive analytics, social media analysis) to proactively detect and respond to fraud schemes?

- We actively employ advanced data analytics to, among other things, monitor transaction/program activity and predict the likelihood of fraud (46%)
- We are currently testing advanced data analytics tools (16%)
- We do not currently employ advanced data analytics, but plan to soon (19%)
- We do not currently employ advanced data analytics, and have no plans to do so (19%)

One way leading organizations attempt to keep pace with fraud schemes is through advanced analytics, which examine patterns for anomalous behavior. Nearly half of respondents say they employ advanced analytics to monitor transaction/program activity and predict the likelihood of fraud.

But roughly one-fifth of respondents are not employing such tools, and the same number say they have no plans to do so.
What do you believe are your organization’s biggest barriers to being able to successfully deploy advanced data analytics tools to proactively detect and respond to fraud schemes? (select all that apply)

- We lack the staff expertise (i.e. data scientists who can manage the analytics tools) - 42%
- We lack the technology tools (i.e. behavioral analytics, predictive analytics) - 33%
- We lack the financial resources to invest in new tools and skills - 30%
- We lack senior management/the board’s support to explore these new tools and skills - 29%

What is the biggest barrier to successfully deploying advanced analytics tools? Skills. Forty-two percent of respondents say their organizations lack the staff expertise – data scientists who can manage the tools.

Another 33 percent lack the tools, while 20 percent say they lack the financial resources to invest in new tools and skills.

The suggestion is that security leaders need to build a better business case to get management’s attention and interest in anti-fraud analytics.

In the next section, the report takes a deeper dive into today’s top fraud concerns.

*Forty-two percent of respondents say their organizations lack the staff expertise — data scientists who can manage the tools.*
2016 Faces of Fraud

Some alarming statistics about current fraud trends:

• 74 percent of respondents say the number of fraud incidents has remained steady or increased in the past year
• 70 percent say total fraud losses have also remained steady or increased
• 52 percent say it can take days or weeks before a fraud incident is detected

As the following charts reveal, the schemes are not necessarily new – but they are ever more successful and exacting an increasing toll.

Overall, which types of fraud has your organization experienced in the past year? (select all that apply)

The forms of fraud are consistent from year to year, with payment card, skimming attacks and account takeover taking the top spots. With a nod to participation from government agency respondents, information theft and insider fraud also rate highly among the most common schemes.

Oddly, 21 percent of respondents say they did not detect any incidents of fraud in the past year. The operative word there may be “detect.” It isn’t necessarily that fraud did not occur, but rather the respondent organizations’ people or systems failed to spot the scams.
The forms of fraud are consistent from year to year, with payment card, skimming attacks and account takeover taking the top spots.
Survey Results

Which types of fraud do you feel your organization is currently best prepared to prevent and detect? (select all that apply)

As for the fraud schemes that organizations are best-prepared to mitigate, those are consistent as well — account takeover, money laundering and payment card fraud among them. These answers also align with the key regulations with which financial organizations must comply.

In the past year, has your organization (or your customers) been the victim of a fraud scheme (or schemes) that was launched through your network?

Asking whether they or their customers have been victimized by fraud schemes launched through the organization’s network, 60 percent say no. But another 25 percent say they do not know, suggesting that detection might be a challenge.
Which of the following impacts did your organization feel as a result of the fraud? (select all that apply)

- Identities were compromised: 41%
- Account data was tampered with or stolen: 35%
- Financial data was tampered with or stolen: 27%
- Intellectual property was tampered with or stolen: 21%
- Partners/suppliers were also compromised as a result of the fraud: 17%
- Government benefits or payments were obtained fraudulently: 13%

For those respondents who do acknowledge such fraud schemes, the top three impacts are: ID compromise, account data tampered/stolen, and financial data tampered/stolen.

When is a fraud incident involving your organization typically detected? (select all that apply)

- At the point of transaction: 44%
- During account audit/reconciliation: 44%
- When a customer notifies us: 37%
- At the point of origination: 29%

In past fraud surveys, the most popular and growing response to the question “When do you detect fraud?” was “When a customer notifies us.” But that trend is bucked by this survey.

Here, drawing from respondents in finance and in government, the top responses are: At the point of transaction and during account audit/reconciliation (both at 44 percent).

Customer notification comes in third.
Survey Results

How is a fraud incident involving your organization typically detected? (select all that apply) *

- Through automated data analysis or transaction monitoring software (66%)
- Third-party notification (48%)
- Internal whistleblower (39%)
- Third-party investigation (20%)

As for how fraud is detected, that is typically through automated data analysis or transaction monitoring software, according to 66 percent of respondents. Third-party notification is the second choice at 48 percent. Internal whistleblowers place third at 39 percent.

On average, how long do you estimate it takes your organization to uncover a fraud incident once it occurs? *

- Real-time (11%)
- Intraday (within 8 hours) (16%)
- Days (1-7 days) (44%)
- Weeks (8%)
- I don’t know (15%)

This is the distressing statistic. On average, once a fraud incident occurs, 52 percent of respondents say it takes days or weeks to uncover the fraud. Fifteen percent do not even know. Only 27 percent say they can detect the incident within a day or even in real time.

Needless to say, much damage can be done in that time between fraud occurrence and discovery.
On average, how long do you estimate it takes your organization to react, respond and resolve the incident after it occurs? *

- 1-8 hours: 31%
- 1-2 days: 24%
- 3-5 days: 14%
- More than five days: 13%
- I don't know: 13%

Response times are not quite as alarming. Thirty-one percent say they can respond to and resolve a fraud incident in 1-8 hours. Thirty-eight percent can do so within 1-5 days.

Has the number of fraud incidents involving your organization increased, decreased or stayed steady in the past year?

- Increased: 41%
- Remained Steady: 33%
- Decreased: 14%
- Unsure: 12%

As stated at the outset of this section, 74 percent of respondents say the number of fraud incidents has remained steady or increased in the past year.

Only 14 percent record a decrease.
By what percentage have fraud incidents involving your organization increased or decreased in the past year? *

![Bar chart showing percentage increases and decreases in fraud incidents]

As for percentage growth, 27 percent of respondents are unsure. But 21 percent detect an increase of 1-10 percent over the previous year.

Have financial losses linked to fraud increased, decreased or stayed steady in the past year?

![Bar chart showing percentage increases and decreases in financial losses]

In line with increase in fraud incidents, 70 percent of respondents say financial losses linked to fraud have remained steady or increased.

Only seven percent have seen a decline.
Survey Results

By what percentage have financial fraud losses increased or decreased in the past year? *

- 11-20 percent increase: 11%
- 1-10 percent increase: 17%
- No change: 27%
- Unsure: 32%

As for percentage change, 32 percent do not know; 28 percent say the change is at least 1-10 percent.

Beyond the financial toll from the fraud incidents, what non-financial losses did your organization suffer from fraud incidents? (select all that apply)

- Loss of productivity: 45%
- Reputational impact: 44%
- Customer accounts (moved to other institutions): 31%
- Regulatory or other compliance issues (additional scrutiny from regulators or standards bodies): 23%
- No non-financial losses: 29%

But, of course, fraud is about far more than financial losses. Asked about non-financial impact, 45 percent of respondents say they have seen a loss of productivity due to incident response, while 44 percent report a reputational impact. Thirty-one percent say they have seen customers close their accounts and take their business elsewhere.

In the next section, the report focuses on enterprise fraud prevention – specifically, the anti-fraud controls organizations have already deployed.
Enterprise Fraud Prevention

So, what have organizations deployed for anti-fraud controls, and how effective are they? Those are the questions to be answered in this section. At a glance:

- 50 percent of respondents say their controls are above average or superior. At the same time, it also can be said that 50 percent rate their controls at average or below.
- 66 percent say technical barriers are their biggest obstacle to improving enterprise fraud prevention.

Read on to see the full responses.

What grade would you give the efficacy of your organization’s current anti-fraud controls?

- A - superior: 11%
- B - above average: 39%
- C - average: 37%
- D - below average: 8%
- F - failing: 2%
- I - incomplete: 3%

The proverbial glass could not be any better balanced between half-empty and half-full. Almost as many respondents rate their anti-fraud controls above average or superior as they do average or below.

For context behind this mixed message, read the subsequent questions and responses. They hint to the respondents’ true sentiment.

The proverbial glass could not be any better balanced between half-empty and half-full. Almost as many respondents rate their anti-fraud controls above average or superior as they do average or below.
When asked which anti-fraud controls they already have deployed, respondents give the “right” answers. They have deployed those controls their regulatory bodies have asked them to roll out: fraud detection and monitoring systems, transaction limits, IP reputation-based tools, etc.
Survey Results

What do you find most lacking in your enterprise’s current anti-fraud tools? (select all that apply)

- Our systems allow for only limited analytics (45%)
- Our organization and systems are siloed, so we have no view of our customers’ activities across our entire enterprise (43%)
- Our systems exist in a patchwork that inhibits any real-time monitoring and decision-making (36%)
- We cannot do real-time monitoring of customer activity (26%)
- Our tools can impede the customer’s experience with us (18%)

Despite the tools they have deployed, organizations say they are still deficient primarily because their systems allow for only limited analytics (45 percent), or their organizations are siloed and do not allow a consolidated view of customer activity across the entire enterprise (43 percent).

What are the barriers that need to be overcome?

What are your organization’s top two barriers to improving enterprise?

- Technical barriers - our controls do not talk to one another among different parts of the organization (66%)
- Customer experience - we do not want to add any new anti-fraud controls that might in any way impede the customer experience with our organization (42%)
- Cultural barriers - there is no easy way to get a consolidated view of our customers’ activities across all of our channels (41%)
- Regulatory barriers - regulations impede our ability to share sensitive information across different offices and systems (22%)

It’s about the technology, they say. Sixty-six percent of respondents say they are held back by technology barriers – their controls do not “talk to one another” throughout the organization.

Meanwhile, 42 percent say customer experience is the issue – they do not want to deploy tools that create any customer friction.

And 41 percent cite cultural barriers – there is no easy way to get a consolidated view of customer activities across all channels, because the organization is not built to create or support such a view.
Survey Results

Barriers aside, if you could design from scratch a new enterprise fraud prevention platform, what elements would it include? (select three that apply)

- Real-time monitoring of customer activity (71%)
- Behavioral analytics that help improve our ability to detect fraudulent activity (68%)
- Predictive analytics that help improve our ability to predict fraudulent activity (67%)
- A broader view of customer activity across the entire organization and its channels (56%)
- More efficient authentication methods that improve both security and the customer experience (51%)
- Social media analysis to improve our ability to spot relationships that might suggest connection to fraudulent activity (35%)

Given these objectives, the next section looks at resources available to fight fraud in the year ahead, as well as specific spending plans.

Sixty-six percent of respondents say they are held back by technology barriers — their controls do not “talk to one another” throughout the organization.
When financial managers are weighing whether current levels of fraud fall under “acceptable risk,” ... it is especially encouraging to see 98 percent of respondents expecting the same or more funding next year.
2016 Fraud Agenda

The good news is: 98 percent of organizations expect to see the same or greater budget for fraud prevention in the coming year.

Top projected investment: New tools

Read ahead to see which specific tools the survey respondents have in mind.

How do you expect your budget dedicated to fraud prevention to change in the next year?

<table>
<thead>
<tr>
<th>Change in Budget</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase of more than 10 percent</td>
<td>11%</td>
</tr>
<tr>
<td>Increase of 6-10 percent</td>
<td>18%</td>
</tr>
<tr>
<td>Increase of 1-5 percent</td>
<td>32%</td>
</tr>
<tr>
<td>No change</td>
<td>37%</td>
</tr>
<tr>
<td>Decrease</td>
<td>2%</td>
</tr>
</tbody>
</table>

It’s never easy to get resources to fight fraud – not when financial managers are weighing whether current levels of fraud fall under “acceptable risk.”

Therefore, it is especially encouraging to see 98 percent of respondents expecting the same or more funding next year. Thirty-two percent project an increase of 1-5 percent, while 18 percent expect a 6-10 percent increase.

Where do you expect to make key investments? (select all that apply)

<table>
<thead>
<tr>
<th>Investment Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>New anti-fraud tools</td>
<td>65%</td>
</tr>
<tr>
<td>Staff training</td>
<td>61%</td>
</tr>
<tr>
<td>Customer awareness</td>
<td>41%</td>
</tr>
<tr>
<td>New staff</td>
<td>23%</td>
</tr>
<tr>
<td>Third-party resources</td>
<td>20%</td>
</tr>
</tbody>
</table>

In general, these new funds will be invested primarily in new anti-fraud tools (65 percent) and staff training (61 percent).
Which specific anti-fraud technology investments do you plan to make within the next 12 months? (select all that apply)

- Fraud detection and monitoring systems 49%
- Big data analytics 26%
- Enhanced controls over account activities 25%
- Enhanced customer education 25%
- Enhanced control over changes to account-maintenance activities by customers 21%
- Rules-based technology 20%
- Behavior-based anomaly detection technology 20%
- Cross-channel fraud detection 20%
- Device ID 14%
- Fingerprint biometrics for authentication 14%
- Out-of-band verification for transactions 13%
- Internet protocol [IP] reputation-based tools 12%
- Dual customer authorization through different access devices 12%
- Positive pay, debit blocks, and other limits on transactional use 11%
- Out-of-band verification for authentication 11%
- Manual processes to detect online banking anomalies 10%

And specifically many respondents are investing in “more of the same” tools they already have, such as fraud detection and monitoring systems (49 percent), enhanced controls over customer activities (25 percent) and enhanced customer education (25 percent).

The encouraging stat is that 26 percent say they also will be investing in big data analytics, which perhaps will help improve some of the established deficiencies in fraud detection.

In the next and final section, the report comes to some definitive conclusions about the 2016 Faces of Fraud, and then it presents expert advice on how to make smart investments in such new controls as advanced analytics.

*The charts represent the top answers given by respondents*
Conclusions

In setting up this report’s conclusions, it is helpful to look back upon the telling statistics from the introduction:

• 67 percent of respondents say it takes one day or more to uncover a fraud incident once it occurs
• 56 percent say customers and/or partners lack sufficient awareness to protect themselves from socially engineered schemes
• 54 percent are not currently deploying advanced data analytics tools

Those three stats form the foundation of these conclusions:

1. It’s About Detection
The “breach science” today is all about response, and many security leaders want to brag about how they have reduced response time to fraud incidents from days to hours or even minutes. But response is for naught if organizations are still struggling to detect incidents of fraud. It is unacceptable – for the organization and its customers – when it can take days or weeks to detect when fraud has occurred. For security leaders to truly address their fraud challenge, they must go to the source. They must invest in the analytics and monitoring tools to help them improve fraud detection.

2. New Tools Needed
When one matches the list of anti-fraud tools that organizations have deployed vs. the ones they intend to invest in next year, there is far too much similarity. Far too much “more of the same” with continued investments in monitoring, controls and education. If these tools have not been effective in the past, why will they be more effective next year? This report is subtitled “The Analytics Approach to Fraud Prevention,” and that is the direction organizations must pursue. Predictive analytics to better understand where fraud might occur; behavioral analytics to better spot fraud when it does occur.

Of course, the tools are wasted if the talent is not there to maximize them. Which leads to the third conclusion.

3. Help Wanted: Educated Users to Deploy the Tools
While not expressly addressed in this report, many of today’s trickier fraud schemes – business email compromise and account takeover – are launched without a malware component. They rely on good old-fashioned social engineering. And the only way to defeat these schemes is to better educate employees and customers on how to spot and respond to them. At the same time, anti-fraud teams need education on how to use today’s top analytics tools. A new, bright box is just that if the users are not sufficiently trained on how to deploy the analytics and apply the data that comes back. Data science is the new, hot discipline and organizations either need to invest in data scientists internally, or contract with third-party experts who bring these skills to the job.

Next, David Stewart, Shaun Barry and Ian Holmes of survey sponsor SAS will weigh in on how best to put these survey results to work in your organization.
Analytics and Enterprise Fraud Prevention – the Keys to Success

Survey Analysis by David Stewart, Shaun Barry and Ian Holmes of SAS

Note: In preparation of this report, ISMG VP Tom Field sat down with David Stewart, Shaun Barry and Ian Holmes of SAS 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.

Survey Surprises

TOM FIELD: What did you find validating about the survey results? What did you find surprising?

IAN HOLMES: The most surprising aspect from the survey was that 98 percent of the respondents expected to receive the same or increased funding for fraud prevention. What I’m typically seeing is that fraud prevention is under very tight constraints.

Biggest Gaps

FIELD: What do you think that we learned about the biggest gaps in our respondents’ efforts to both detect and then prevent fraud?

SHAUN BARRY: When respondents say today’s fraud schemes are too sophisticated or evolve too quickly for them to keep pace, we get an interesting insight into the gaps our clients face. They certainly appear to have the ability to stop what they know, but they don’t know how to prepare or respond to things they don’t know. It’s an interesting weakness on their part – and an interesting opportunity on our part.

What About Analytics?

FIELD: From this survey, what have we learned about how organizations currently use data analytics to spot – and stop – fraud schemes?

DAVID STEWART: We’re at an interesting point in the industry with response to data analytics. While several tried and true techniques are effective, there’s an increased interest in newer machine-learning capabilities. Artificial intelligence and machine learning has the potential to leverage new strategies without needing specialized skill sets. A so-called “citizen data scientist” can submit a problem set of data to an algorithm that will magically make the best decisions for them.

Part of the reason that so many institutions find this so appealing is because they lack a good cultural understanding of the types of analytic techniques that would be most effective for various types of fraud. For types of fraud where a lot of known fraud incidents already exist, supervised learning like neural networks can be very effective. In contrast, black swan events, like CEO spear-phishing, may be more effectively quashed using other techniques. Ultimately, organizations need to be pragmatic about when and where various techniques are deployed.
The Confidence Quandary

FIELD: One key takeaway from the survey is that only a third of respondents report they have high confidence in their organization’s abilities to detect and respond to fraud. Drawing from your own experience with your customers, what challenges most undermine security leaders’ confidence?

BARRY: The “unknown unknowns,” to use a Donald Rumsfeld term. They know what they detect today, but they also know from customer feedback and from the losses they experience, they don’t catch everything before it happens. So, it gets back to that concept of, “I don’t know. The schemes are coming so quickly and evolving so fast and are so sophisticated that I can’t keep up.” That contributes significantly to that lack of confidence.

HOLMES: Although many clients and financial institutions claim to be customer-centric, their organizations are still very siloed – not only in their fraud detection capabilities, but also in their data availability and visibility in seeing across data that goes into their institutions.

Also, the amount of data risk has become baffling for them. They may use Access and Excel or, in some cases, more capable analytic software from a business perspective, but they find it extremely difficult to gain a holistic understanding of all the data coming in and where they can squeeze out benefits from the data scrum.

STEWART: Fraudsters’ pace of innovation has outstripped the pace of innovation in the corporate sector. There’s just no comparison. Just look at things like ATM skimmers and the recent SWIFT wire fraud incidents that were allegedly perpetrated by state-sponsored groups of hackers. It’s daunting.

Over the last few years, a lot of that innovation has occurred in areas like authentication and biometrics that are designed to make mobile and online payments more secure. It goes back to Ian’s point about lack of visibility into the payment authorization stream or across the view of the customer. If you lack that visibility, you’re limited in the efficacy in that type of innovation to counteract the fraudsters.
Analytics & Gaps

FIELD: Nearly half of respondents now employ some form of advanced data analytics, but nearly as many say they lack the expertise or the tools to truly maximize these solutions. What gaps do you typically see with regard to data analytics, and how are organizations filling those gaps?

STEWART: The biggest barrier continues to be from a skill sets perspective because the demand for analytic talent has become so great. It’s one thing to find quantitative scientists, but it’s difficult to find quantitative scientists who understand, say, a certain government sector or commercial banking.

We’re interacting with some very large, sophisticated clients, and it’s always amazing to me that, even though they do have resources, their bandwidth is constrained with the demand of project workload they’re under. That’s what leads them to companies like SAS that not only provide the analytical technologies, but provide the subject matter experts with years of experience in a certain industry sector to show how to apply those tools to reduce fraud. And so I continue to be amazed that clients often ask for an open-box environment, so they can build models that can be validated, tuned and optimized. More often than not, we teach them how to be self-sufficient – and more often than not they’ll come back and ask us to augment some of their analytical strategies.

Incidents & Losses

FIELD: It’s clear from the survey results that both the number of incidents and the financial losses are mainly increasing. No one’s really reporting a decrease. What does this say then about the anti-fraud tools that organizations have traditionally deployed? Is it too simplistic to say that they’re just not working and they’re just not sufficient?

HOLMES: I would say this comes back to, 1) the utilization of the fraud detection capabilities they have, and being able to apply those. And 2), maybe, potentially, bad decisions where they depended upon a vendor’s capabilities, and that vendor were not able to change the way their systems identified fraud. So it’s left the client behind in what their capabilities are.

BARRY: I would echo that. In some ways, it’s about the tools, and in some cases tools may not be able to keep up with the innovation that fraudsters are showing. But sometimes it’s just the way that those tools are configured. You may have the right tools, but you’re not telling that technology what to look for and the types of behaviors that might be out there.

Overcoming Technical Hurdles

FIELD: Respondents cite that the biggest barriers to improving their fraud defenses are technical. How does this match what you commonly see with your customers?

BARRY: Most of our clients have a decent sense of what should be, as opposed to what is today. And they see how they could improve things from a technical perspective. But that doesn’t tell the complete picture. Oftentimes, particularly in government and healthcare, it’s a combined question of technical barriers and then, frankly, the human resources that an organization has or hasn’t have to effectively pursue fraud and improve fraud defenses. So, the respondents only gave half of the answer – at least in my experience – to the biggest barriers they may have.
Moving Forward

**FIELD:** Let’s talk about technology. What are the must-have tools organizations need to improve fraud detection and response?

**BARRY:** You need the ability to get data from multiple sources and bring it together. Therefore, you need data management technologies and advanced analytics technologies that handle multiple forms of analytics – including predictive models, link analysis, machine learning techniques, and anomaly detection – at the same time. These technologies would then supplement basic conditional logic and business rules that most of our clients use today. Finally, these technology tools must present their results in an approachable way so that our clients’ investigators can understand them and act on those results.

Where to Find the Skills?

**FIELD:** Where can organizations gain and retain the necessary skills needed to maximize the tools and capacities that they need now?

**BARRY:** Organizations need to figure out whether fraud detection and prevention is a core competency or something that would make more sense to outsource to a qualified vendor. For example, if a government agency focuses on tax, revenues and compliance, it would view fraud prevention as a core competency because that’s its job. In contrast, the primary task of a private healthcare payer is to analyze and pay claims, so fraud prevention, while obviously important, is not its core competency.

So, it will be a combination of increasing internal skills and recruiting, which means changing pay scales, and then outsourcing to competent vendors.

Justifying Investments

**FIELD:** What advice do you give to security leaders to help them justify additional anti-fraud investments?

**STEWART:** For financial services, look at the loss revenue or the opportunity cost of revenue and profitability, due to higher false positive rates. It’s pretty easy to make a case that customer experience is arguably the No. 1 driver because you want to alienate fewer people.

**BARRY:** On the government and healthcare side, we run across this all the time. In the case of healthcare, we could find fraud, abuse and waste in healthcare claims until the cows come home. But healthcare payers have a difficult time in monetizing those alerts because they have not yet moved to a pre-payment type of analysis. They can’t easily go back and do a pay and chase approach. Instead, they need to stress that no losses are acceptable because they are so great. The estimates for fraud, waste and other abuse are anywhere between 10 to 30 percent of healthcare expenditures, all of which are hard to justify as being acceptable.

In government, it’s much easier to justify this investment because nobody wants to be perceived as being an inefficient government program. Therefore, you want to appeal to the public good, as well as reputational risk. In fact, reputational risk can be a very powerful incentive because once you’re able to push the bad guys over to your competitors, you gain a pretty sterling reputation among your customers.
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.