IDC Special Custom Study: Cyber Security Strategies & Approaches, Big Data Usage, and Cyber Profiles of US Industrial Organizations in 2016

Earl Joseph, ejoseph@idc.com
Steve Conway, sconway@idc.com
Bob Sorensen, bsorensen@idc.com
Kevin Monroe, kmonroe@idc.com

STUDY BACKGROUND AND MOTIVATIONS

The present study is the follow-on to a less-extensive 2015 study conducted for the clients, to identify cybersecurity practices in the U.S. private sector—from best to worst practices.

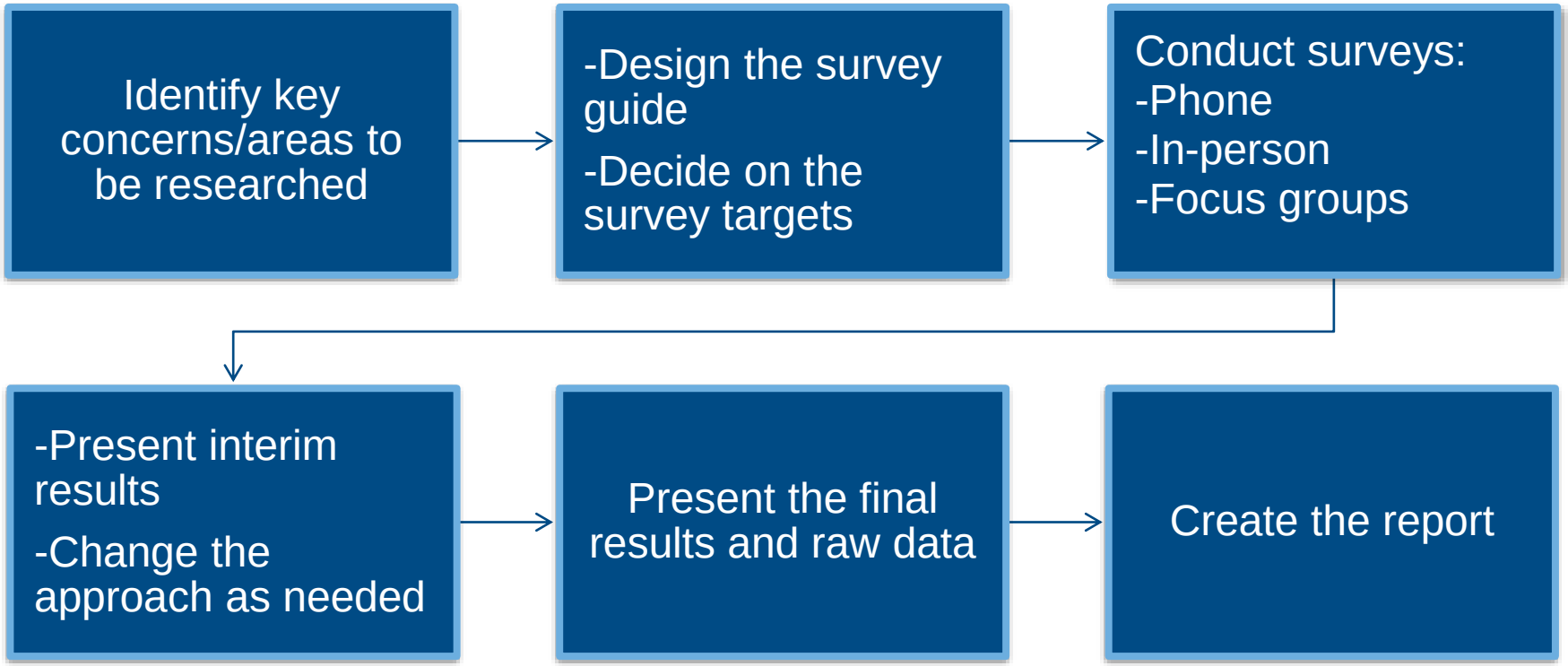
- The 2015 study revealed a wide spectrum of attitudes and approaches to the growing challenge of keeping corporate data safe.
  - While the minority of cybersecurity best practitioners set an admirable example, the 2015 study findings revealed that most U.S. companies today are underprepared to deal effectively with potential security breaches from outside or inside their firewalls.
- There was a frequently voiced belief among the interviewed firms that they would inevitably be breached, yet many of the firms seemed content to wait until then to focus harder on cybersecurity.

STUDY OVERVIEW

This current study zeroed in on best practitioners and their cybersecurity practices, with special emphasis on large firms in the financial services and technology sectors—because these sectors were cited in the 2015 study as best practitioners, and because their need to protect very-high-value data is a requirement shared by the clients.

- Interviewees extended beyond these two sectors to include other best practitioners and, for contrast, a number of large organizations assumed not to be best practitioners.

IDC Study Methodology:
Asking the Right Questions of the Right People Leads to the Most Relevant Information



Survey Respondents

In total 62 U.S. organizations were surveyed in this study. IDC conducted two types of interviews:

- One-on-one interviews of 25 organizations, in person or by phone
- Focus groups with 8 to 10 participants each. These were held in New York, Chicago, Boston, and San Francisco. A total of 37 organizations participated in these focus groups.

IDC was able to recruit a stellar lineup of known-name private sector firms to participate in this study.

Job Titles of Respondents

Which of the following best reflects your title in your organization?		
	Number Citing	Percent Citing
VP IT & SVP IT	10	16%
Director IT Security	8	13%
CISO	7	11%
Director of IT	7	11%
Manager IT	6	10%
CIO	5	8%
IT Security Manager	3	5%
VP Operations	2	3%
Other Titles	14	23%
Total	62	100%

Source: IDC, 2016

Industry/Sector of Respondents

	Number Citing	Percent Citing
Financial Services/Insurance	23	37%
Healthcare/Life Sciences	7	11%
Entertainment/Media/Publishing	5	8%
Manufacturing	5	8%
Consulting Services	4	6%
Business Services	3	5%
Retail	3	5%
Distribution Services (security products)	2	3%
Education	2	3%
Oil & Gas	2	3%
Transportation	2	3%
Defense Contractor	1	2%
Nonprofit organization	1	2%
Real Estate	1	2%
Utilities (natural gas distribution)	1	2%
Total	62	100%

Key Takeaways

The cyber teams reported that in the past 2-3 years, they have quickly evolved from "sleepy village" operations to busy, mission-critical enterprise units driven by escalating cyber threats.

- Cyber teams have had to come up to speed quickly using proven tools and approaches that few of the respondents have had time to investigate and implement newer advanced analytics ("Big Data") capabilities.
  - Almost no one had used advanced analytics for cybersecurity long enough to measure their effectiveness.
- The rarity of data scientists who can also do cyber is a major stumbling block.
  - Nevertheless, most respondents expected to use Big Data capabilities in the future and said that cyber security software vendors will be the ones to integrate these capabilities into their off-the-shelf products

Fit Within Organization

Cyber teams are often (though not always) isolated within their employer organizations and are seldom connected, for example, to colleagues performing analytics on operational business data (payroll, HR. etc.).

Cyber teams typically are directly accountable to the CEO and board of directors, for two reasons.

- The CEO and board have ultimate responsibility for the corporate reputation, corporate risk management, and protecting critical business data.
- The CEO and board members can be sued individually for alleged mismanagement, which may include failure to protect corporate data against breaches.

Over time, enterprise IT operations and IT security will converge, breaking down the isolation between securing operational business data and assuring its availability and integrity.

Fit Within Organization

As a consequence of the solid-line reporting of cyber teams to the CEO and board, respondents almost without exception said that when they request additional unbudgeted funds for cybersecurity during the fiscal year, in most cases the requests are quickly approved by the CEO.

- ROI considerations are generally minimal.
- Managements seem to trust their cyber teams when it comes to budget requests and mid-year requests for additional funds—within reason.

Fit Within Organization

As more resources are migrated to the cloud, business teams will demand unfettered access to many of these resources and a seamless flow of data across the IT infrastructure creating privilege management, authentication and authorization challenges that must be met

Breach Plans

Everyone had a breach response/recovery plan, but what's in the plans varied widely.

- Some firms focused 100% of their plans on IT procedures, while for other firms, IT directives represented less than 20% of the contents of the plans—with most of the content devoted to legal and publicity matters.

The public relations sensitivity was not surprising, as the 2015 study showed that cyber best practitioners considered protecting the company's reputation even more valuable than protecting the data itself.

- For them, losing high-value data is an addressable problem, but losing your good reputation can quickly put the company out of business.

Breach Plans

Security functionality is increasingly being embedded into applications, business platforms, and cloud services, reducing the risk of the exposure or theft of critical corporate data.

- IT is increasingly being outsourced to managed services providers and enterprises are engaging with managed security services providers to protect their most critical assets.
- This results in a variety of new roles within the organization to manage these relationships, oversee compliance, respond to security incidents and maintain consistent policies and enforcement mechanisms.

Frameworks

Most of the respondents first reviewed existing frameworks (NIST, ISO, et al.) and then used elements of multiple standard frameworks, along with their own additions, to create custom frameworks for their employers.

- Hence, the standard frameworks typically provide a starting point but they are rarely used in standalone fashion or in their entirety.
- Many respondents viewed their custom framework as a "secret sauce" whose recipe needed to be closely guarded.

Questions about capability maturity models caused more head scratching (“what’s that?”) than any other answer.

- There was little understanding of what this term means.

Security Frameworks

What security framework/paradigm do you use in your big data infrastructure?		
	Number Citing	Percent Citing
NIST	5	26.3%
Leveraging our regular CSF/CIA triad	4	21.1%
ISO	3	15.8%
SANS/CIS Top 20	2	10.5%
COBIT	1	5.3%
MPAA	1	5.3%
HITRUST CSF	1	5.3%
FFIEC CAT	1	5.3%
OWASP	1	5.3%
Total	19	100.0%

Note: 19 sites responded to this question.

Source: IDC, 2016

Use of Big Data Analytics for Cyber Security

In the rush to face escalating threats in the past 2-3 years, few firms have had time to apply Big Data tools to cybersecurity.

- Best practitioners typically equip their human talent with long-standing tools today.

A small contingent of known-name firms are at the early stages of Big Data use for cybersecurity. Some other firms are pioneering Big Data use for fraud detection and remediation.

- Big Data capabilities are still in their infancy within the U.S. private sector --a small number of firms are farther along).

Using Big Data for Cyber Security: Tools Used

Do you use big data in any of your cyber security operations? If yes, what tool?		
	Number Citing	Percent Citing
Splunk	11	28.2%
Sumo Logic	1	2.6%
EDB PostgreSQL	1	2.6%
LogRhythm	2	5.1%
Tableau	1	2.6%
Nexpose Rapid7	1	2.6%
CrowdStrike	1	2.6%
SolarWinds	1	2.6%
Microsoft SQL	1	2.6%
Not specified	19	48.7%
Total	39	100.0%

Using Big Data for Cyber Security: Where Its Used

Do you use big data in any of your cyber security operations? If yes, where?		
	Number Citing	Percent Citing
Log/data aggregation and analysis	9	33.3%
Threat/security analytics	8	29.6%
Real-time monitoring/data collection	6	22.2%
Pattern recognition/sig/risk detection	2	7.4%
Regulatory-based Analytics	1	3.7%
Log management	1	3.7%
Total	27	100.0%

Note: 27 sites responded to this question.

Source: IDC, 2016

KPIs

Even best practitioners today are largely on their own when it comes to establishing key performance indicators (KPIs) for cybersecurity, because no widely accepted set of standard KPIs exists yet.

- Most U.S. firms rely almost entirely on metrics such as the number of thwarted attacks and time-to-identification of attackers.
- Best practitioners use these quantifiable metrics only as a starting point and go one from there to look at factors such as forensics outcomes and the impacts of cyberattacks on the business's financial performance and reputation.

Threat Sources

There was generally equal concern about outsider and insider threats, although some respondents believe insiders have the potential to do more damage because of their greater access to high-value data.

- There was strong consensus, however, that the posture should be to trust no one and work to ensure that your security regimes prevent inappropriate access by all parties.

BYOD is now a given. Cyber security needs to deal with that reality.

- But most employees are willing to have security software loaded onto their phones---within reason.
- Role-based access (RBAC) is common.

Internal Sources of Threats

Response	Number Citing	Percent of Responses
Employees (intentionally/knowingly)	22	38%
Employees (unintentionally/unknowingly)	21	36%
Policy	4	7%
Partners	4	7%
Vendors	3	5%
Technical	2	3%
Contractors	2	3%
Total	58	100%

Source: IDC, 2016

External Threats

What are the main external threats to the organization via cyber actors?		
	Number Citing	Percent Citing
Cybercrimals/APTs	29	39.7%
Malware	13	17.8%
Phishing schemes	12	16.4%
Automated attacks	7	9.6%
Foreign governments/organized crime	4	5.5%
Corporate espionage	3	4.1%
	3	4.1%
	1	1.4%
Unknown traffic	1	1.4%
Total	73	100.0%

Note: There were 73 responses to this question.

Source: IDC, 2016

Threat Intelligence Sources

Most respondents subscribe to external suppliers of threat intelligence, which is supplied on a monthly or more frequent basis.

- In some industries, such as manufacturing, cyber officials from multiple companies belong to local or regional associations that meet frequently (e.g., monthly) to exchange new cyberattack information and experiences on a pre-competitive basis.

Frequency of Threat/ Vulnerability Data Reception

Frequency	Percent Responding
Real time/constantly/hourly	27%
Multiple times per day	6%
Daily	56%
Multiple times per week	6%
Weekly	11%
Bi-weekly	5%
Monthly	8%
Every 6-8 weeks	3%
Quarterly	5%
Annually	2%
Non-scheduled/as needed/as threat/vulnerability is discovered	10%
Not often enough/notifications needs to be more proactive vs. reactive	3%

Source: IDC, 2016

Best Practices

The best practitioners view cyber security as a human-vs.-human challenge, where having the best people is more important for combatting "bad guys" than having the right technology.

- This also explains why the best practitioners tend to hire ex-law enforcement people rather than IT people to head forensics.

It's not the procedures or the technology that matter most, it's the personnel that drive the system.

- The procedures they use are merely second-order effects of having the right people.
- The cyber experts we spoke with all expressed deep commitment to their employers' missions.

<u>All had adjusted their philosophies to meet the overall business requirements of their company…not the other way around.</u>

IDC Opinion

It is a near-certainty that cyberattacks will continue to escalate in frequency and sophistication, and that attackers will make increasing use of advanced analytics methods.

- IDC believes that to avoid losing ground to these threats, best practitioners will also need to apply Big Data methods in their cybersecurity operations.
- It will take longer for these methods to find their way into the majority of U.S. companies.

IDC Opinion

The dissemination of the cybersecurity function will embed threat awareness—and cybersecurity responsibility—directly into the work lives of nearly all employees.

- Assuming that the dissemination trend spreads to firms that are not best practitioners today, as IDC believes is likely, this trend could help most U.S. companies that are substantially underprepared for the cybersecurity threats they face.
- The dissemination trend will create a greater need for cybersecurity education and training; if the majority of employees will need to have cyber awareness and responsibility, either universities or employers will have to prepare them for this.

A Cyber Security Safe Haven? A federal initiative may be needed to spur and support this activity.

Questions?

ejoseph@idc.com

sconway@idc.com

bsorensen@idc.com

kmonroe@icd.com

IDC
Analyze the Future