2016 Cybersecurity Tactics Snapshot

Arraya

Introduction

Image searches for the word “hacker” turn up pages of hoodie-wearing figures lurking in the shadows with only a laptop for company. It is a striking representation – and one that couldn’t be further from the truth.

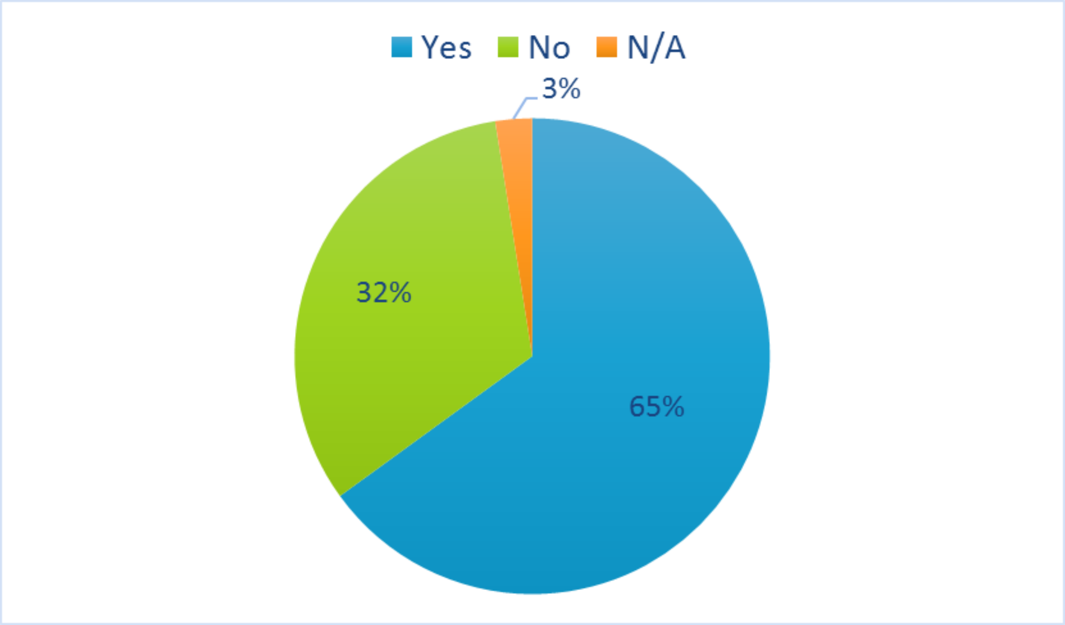
Cybercrime has ballooned into a billion-dollar industry. Modern cybercriminals are organized, well-funded, and not afraid to try something new – or revisit something old – in terms of their tactics. As such, they have gotten very good at keeping their counterparts in cybersecurity guessing.

Better, more connected tools. An organization-wide commitment. These are indispensable pieces of any strategy to fight today’s cybercriminals. Another essential element is learning from what others in the field have tried and what they have experienced. That mindset led to the creation of the Arraya Solutions *2016 Cybersecurity Tactics Snapshot*.

We surveyed attendees of our 2016 Tech Summit about how their organizations approach cybersecurity. This group included IT professionals representing all organizational levels and a diverse collection of industries. The insight they provided demonstrates how these leading organizations are working to ensure their data is secure.

Part I: Data Breakdown

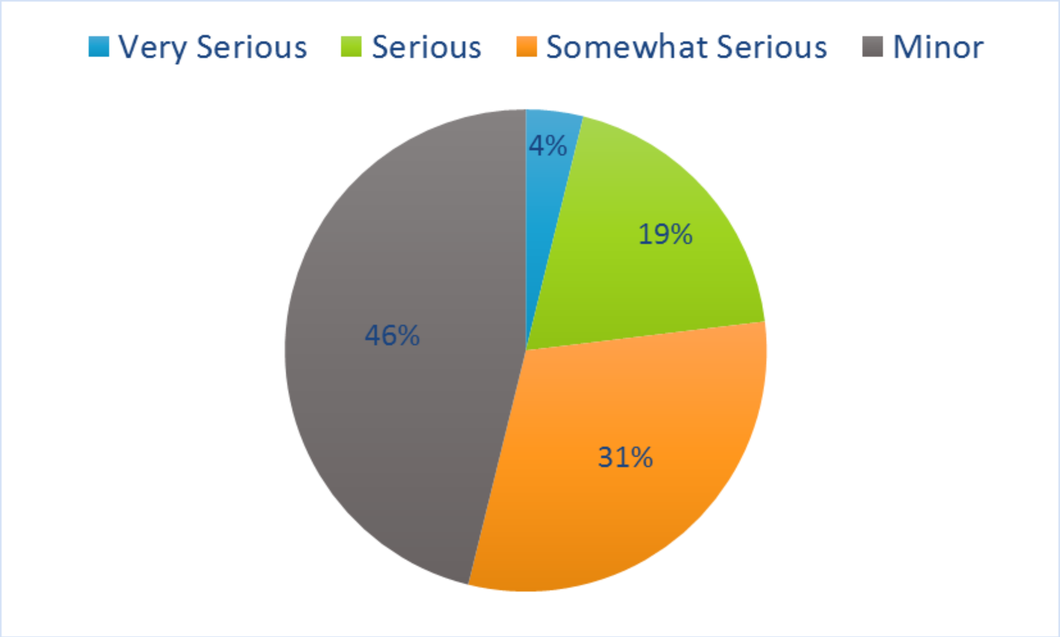
Figure 1: Has your business dealt with a security incident in the past 12 months?



Cybersecurity is top of mind for many organizations in our study – perhaps because they suffered an incident and lived to tell the tale. Figure 1 shows 65% of respondents acknowledged their business has dealt with a security incident in the last year. That figure is twice the size of those who have been lucky enough to avoid a breach over the past 12 months (32%).

It can take months to detect a breach. All the while, an unwelcomed third party is able to peruse the corporate network, accessing whatever data seems most interesting or valuable. This is why, as important as external defenses like firewalls are, organizations must also have internal trip wires set to alert them to criminals who have already gotten in.

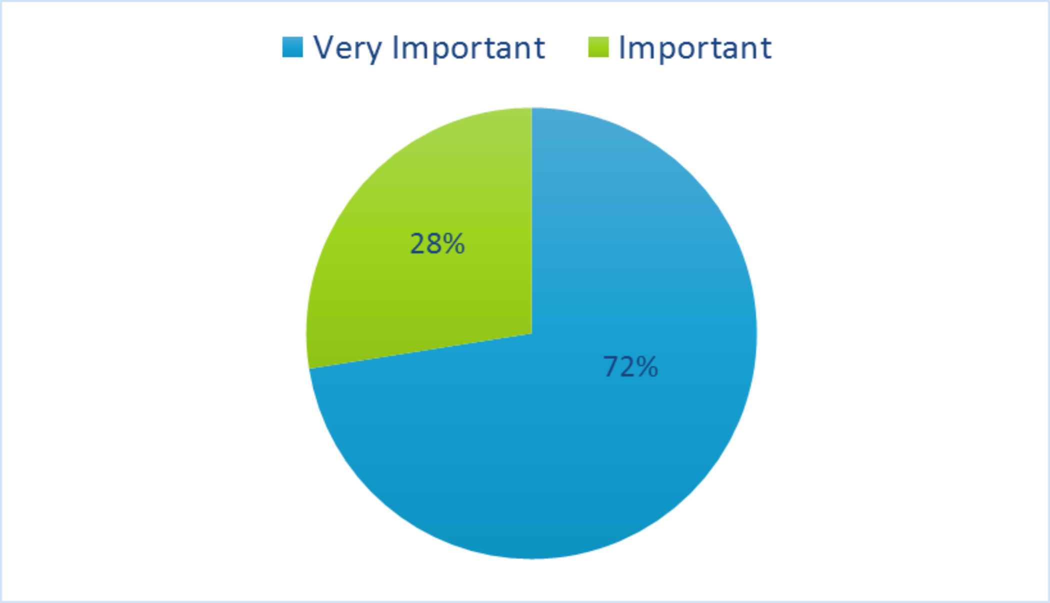
Figure 1a: If yes, how would you describe the extent of the breach or attack?



The good news for organizations? The security incidents they had to contend with mostly registered on the low end of the severity scale. Of those who said they'd dealt with an incident, 46% described the intrusion as "Minor." Meanwhile, 31% of those surveyed believed the incident to be merely "Somewhat Serious." However, for 23% of participants, their incident(s) fell into either the "Serious" or "Very Serious" category.

Security incidents have a way of snowballing. If left unchecked, something that started in the "Minor" category can rise up the ladder. The speed with which this can happen has made solutions that enable real-time or near-real time detection and response critical.

Figure 2: How important do you believe security is to your organization's business strategy?



It's encouraging to see 100% of organizations surveyed identify security as at least an "Important" part of their business strategy. Obviously, it would be even more encouraging to see 100% of organizations describe it as "Very Important," instead of having 28% hold out at the "Important" level. Still, this shows businesses are off to the right start.

The fallout from a security incident can be severe, in terms of the financial hit and the damage to an organization's reputation. As a result, the primary goals of the cybersecurity side and the business side align more closely than either might realize. Good communication and regular facetime between these teams are necessary for both to achieve their goals.

Figure 3: How confident are you in your organization's ability to bounce back quickly from a security incident?

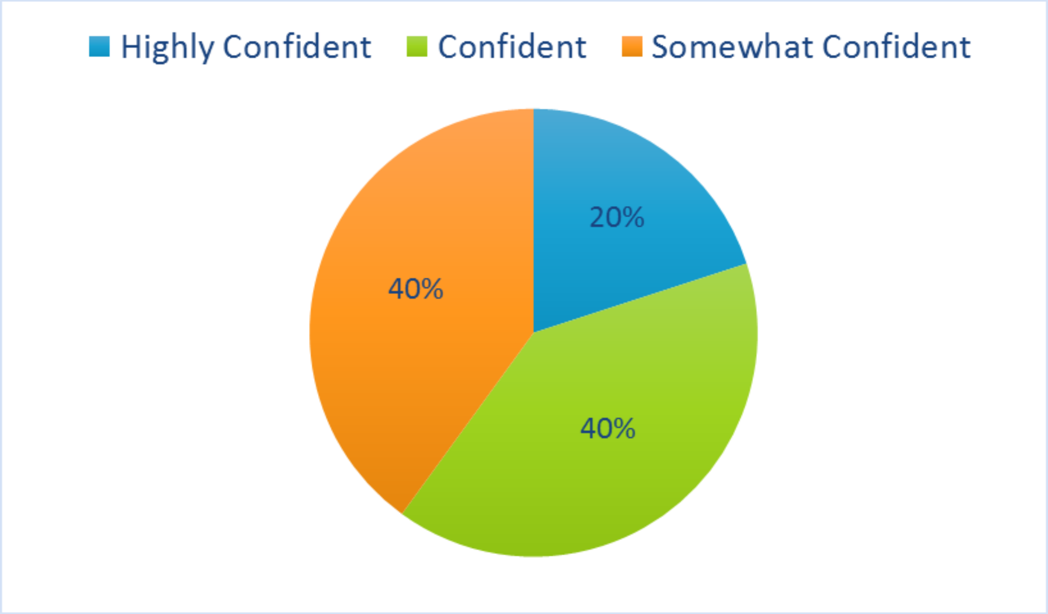
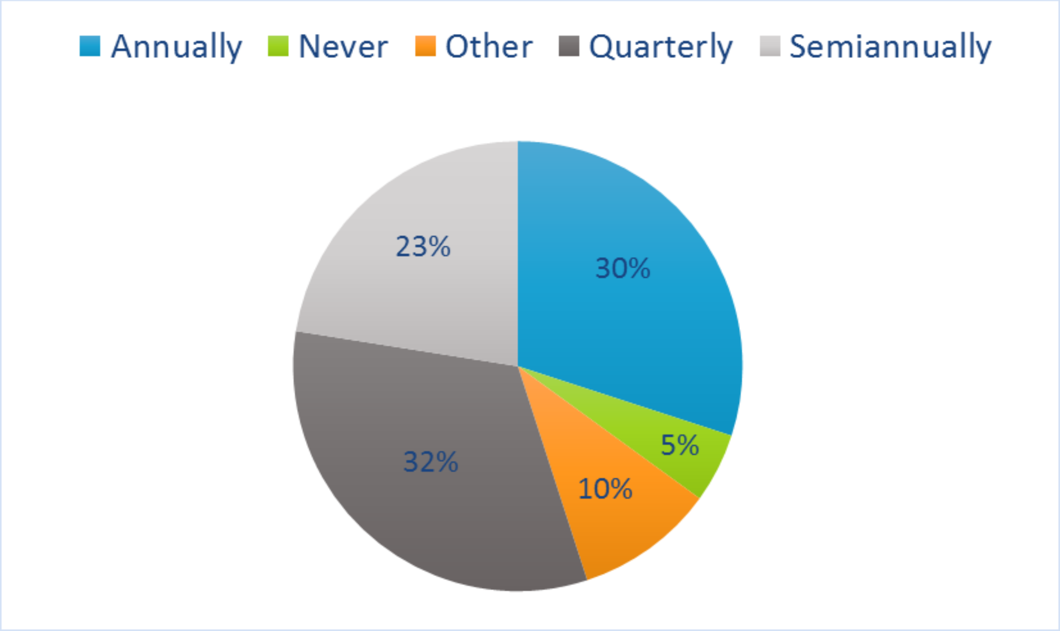


Figure 3 shows a tie between respondents who felt "Confident" (40%) in their ability to bounce back following a security incident and those who were only "Somewhat Confident" (40%). Both figures blew past the "Highly Confident" crowd, which came in at just 20%. That doesn't paint the rosiest picture of organizations' disaster recovery capabilities.

Confidence doesn't only stem from deploying best-of-breed security solutions. It also comes from testing those solutions to ensure they were deployed correctly, have been properly maintained, and will react the way they are supposed to in the face of a threat. Assuming everything will go as planned is an open invitation for disaster.

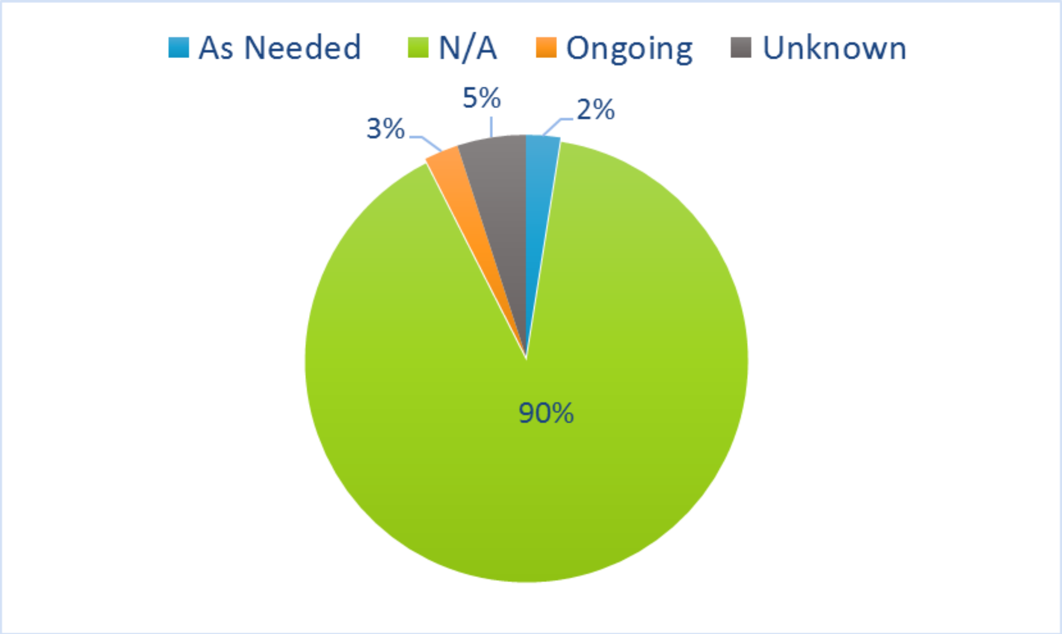
Figure 4: How often does your business review its IT security policies and practices?



According to our findings, businesses are doing a good job of ensuring their cybersecurity policies and procedures are up to the challenge presented by cyber crooks. Roughly 1-in-3 (32%) said their organizations review security policies and procedures "Quarterly." From there, 30% said they do so "Annually," while 23% said "Semiannually."

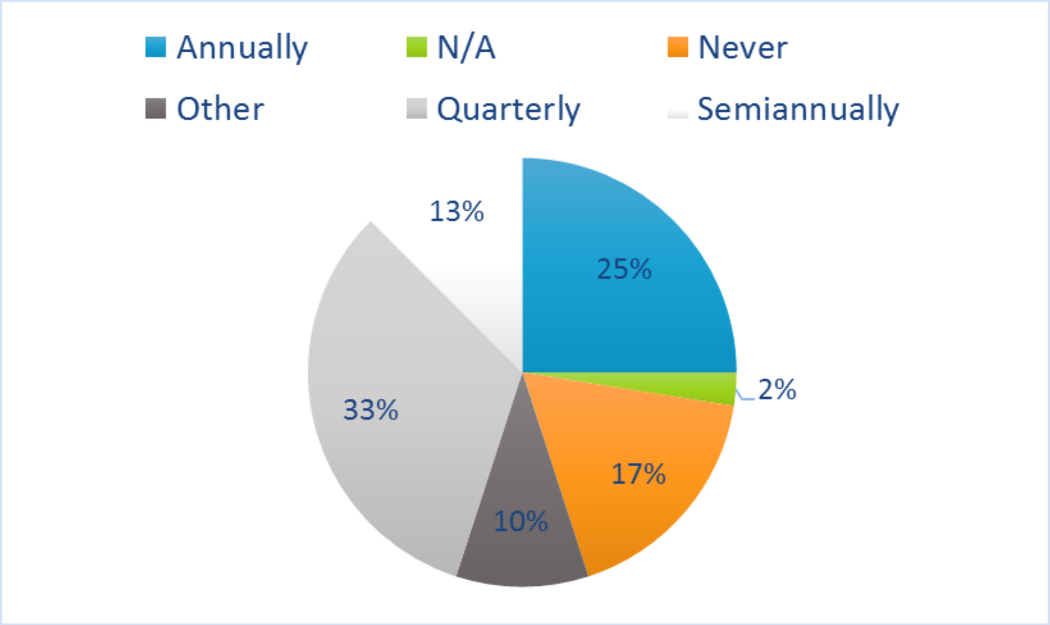
The tactics used by cybercriminals are constantly evolving. This fluidity requires an equal response from those tasked with cybersecurity. Reassuring as they may be, these results may not be typical across a broader spectrum as internal IT teams aren't known for having an abundance of free time. Still, if time isn't made for reviewing and adjusting organizational security policies, it is almost the same as giving cyber crooks a head start.

Figure 4a: If "Other," please explain.



IT pros whose cybersecurity policy review practices didn't fall into one of the above categories were invited to write in an answer of their own. The results spanned both positive ("Ongoing"), and negative ("Unknown"). One answer that stood out was "As Needed." This response could indicate an "if it ain't broke, don't fix it" mindset. As was already mentioned, the damage done when something does break can be severe. Businesses can avoid those costs by instituting a regular review process to stay in front of potential issues instead of reacting to them.

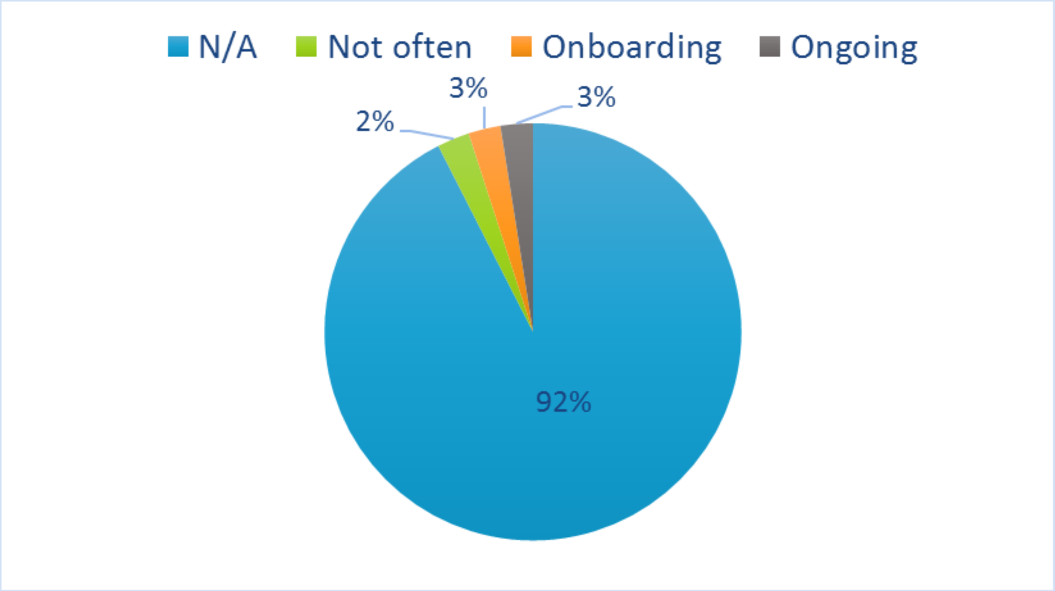
Figure 5: How often does your business review IT security best practices with end users?



End users have a vital role to play in the fight against cybercriminals – provided they have the tools and knowledge at their disposal to do so. When it comes to ensuring users have those tools, respondents were all over the board. Roughly 33% of organizations said they review cybersecurity best practices with end users “Quarterly.” The next most popular response was “Annually,” which came in at 25%. On the downside, 17% of organizations said they “Never” review these best practices with end users.

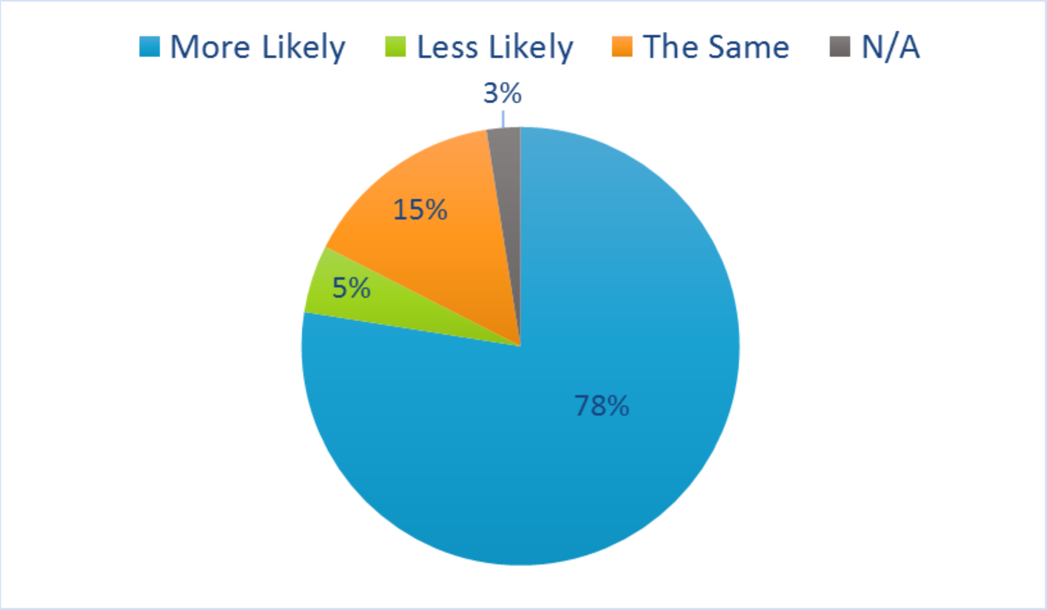
While proper training can make end users a valuable asset in this fight, a lack thereof can make them a tremendous liability. Without it, they’re more likely to fall victim to common cybercrime tactics such as phishing and social engineering. Again, this type of training requires a time commitment from IT, but the risks of not doing it are too great to ignore.

Figure 5a: If other, please explain.



IT pros whose end user training processes didn't align with any of the above schedules were asked to write in their own response. Their answers ranged from "Not Often" to "Ongoing." Another answer was "During Onboarding." There is certainly value in providing incoming employees with cybersecurity training. However, veteran employees aren't immune to cybersecurity threats. Positive habits must be reinforced and new attack vectors explained. This is why ongoing training is so essential.

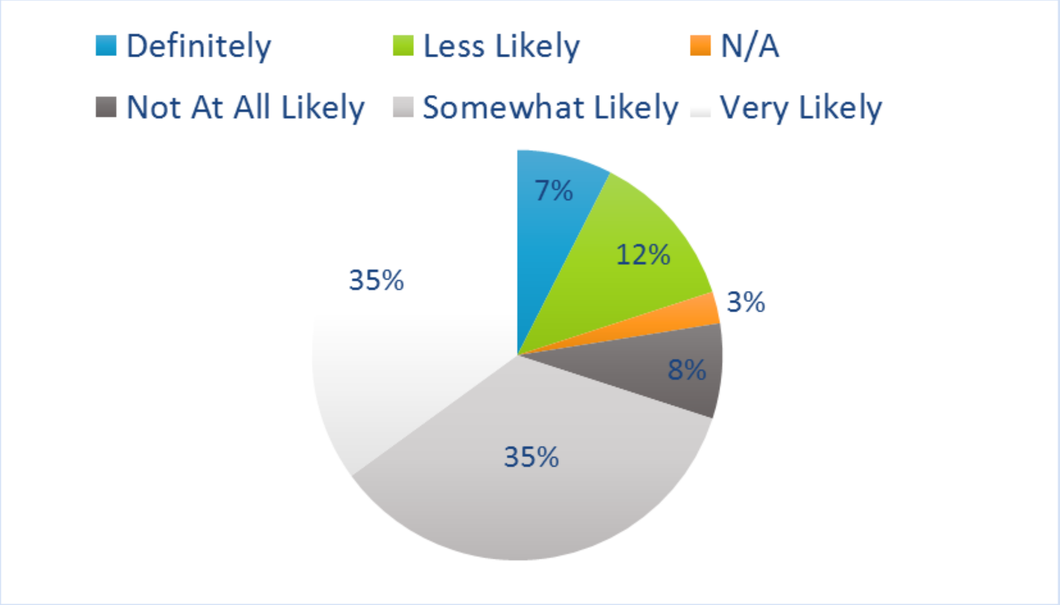
Figure 6: How likely are you to do business with an IT solution partner that knows and understands security (vs. one that doesn't?)



Organizations have a laser focus on security – and they want to do business with partners who can say the same. According to our findings, 78% of businesses are "More Likely" to do business with an IT solution partner who knows and understands security versus one who doesn't. Just 15% of respondents said security expertise doesn't factor in to their IT partner selection process.

Whether they work in IT or some other vertical, third party vendors can pose a risk to an organization's cybersecurity. High-profile data breaches can have their origins in the data centers of a much smaller, inconspicuous third party. In today's business world, organizations need partners who know security, know their industry, and will work with them to ensure continued data safety and overall compliance.

Figure 7: How likely are you to leverage an IT solutions partner to help manage the security of your network, systems, and information?



Cybersecurity is a big job, one that can leave little time for IT's other responsibilities. In order to preserve IT's ability to be proactive and forward-thinking, many organizations have entrusted a third party to manage the tools that protect their environments. Nearly 4-in-10 (35%) said they were "Very Likely" to do so. Another 35% said their organizations were "Somewhat Likely" to do so. A mere 8% of respondents said they were "Not At All Likely" to enlist the help of an IT partner to help manage their security investments.

Security is a major concern for IT pros, but for most, it's not their only focus. In order to maintain a competitive advantage in their industries, businesses must adopt a forward-thinking approach to technology. Finding time to investigate the latest solutions to hit the market while also handling the day-to-day needs of IT environments can stretch onsite IT teams thin. By freeing IT teams of the burden of routine tasks like maintenance and updates, it allows them to focus on how to drive the business forward today, tomorrow, and five years from now.

Part II: Observable Trends

As we crunched the data for the *2016 Cybersecurity Tactics Snapshot*, a number of interesting trends began to crystalize. We wanted to share these findings as well as explore the impact they could have on businesses' cybersecurity policies.

- **Regular reviews make for highly confident companies.** Of the companies who described themselves as "Highly Confident" in their ability to bounce back quickly from a security incident, 75% perform Quarterly reviews of their IT security policies. Of those same Highly Confident organizations, 63% perform Quarterly cybersecurity policy reviews with end users.

- **Fewer reviews means less confidence.** Meanwhile, organizations who described themselves as being “Somewhat Confident” in their ability to bounce back quickly from a cyber security event, were more likely to review their security policies Annually (38%) or Semiannually (38%). As for reviewing cybersecurity policies with employees, the answers varied, but the majority of “Somewhat Confident” companies (25%) never made time for these reviews.

- **Organizations who have been breached make more time for reviews.** Companies who have experienced a security incident are eager to avoid a repeat incident, evidenced by the fact that they are more likely to review their security policies at least twice a year. According to our research, 62% of companies who have been burned in the past 12 months currently review their polices at least Semiannually. In addition, companies who have survived a cybersecurity incident also make more time to review policies with end users. Nearly half (46%) of the IT pros we surveyed whose organization has been breached review policies with end users at least twice a year.

- **No breaches translates to fewer reviews.** Organizations who haven’t been breached in the past 12 months and who haven’t dealt with the fallout are prone to being less careful. Only 38% of these businesses currently review their security policies at least twice a year. Also, just 38% review policies with end users at least twice a year. Another interesting trend among companies who have avoided a breach: 31% say they never review policies with their end users. Considering the target most cybercriminals have placed on the average employee, skipping training seems a risky plan.

- **Companies are careful about third parties following a serious incident.** For respondents whose organizations have suffered a serious cybersecurity incident – or worse – in the past year, security knowledge plays an important part in their IT partner selection process. Roughly 83% of these businesses said they would be “More Likely” to do business with an IT partner who understands security compared to one who doesn’t.

Part III: Conclusion

Our perception of hackers isn't the only thing that must change. The cybersecurity landscape is has a whole is constantly changingin motion and businesses must change with it. Businesses whose approach to cybersecurity lack the flexibility to keep pace with cybercriminals run the risk of paying a steep price. The costs of a security incident aren't limited to detection and remediation. Instead, they can be felt long after a breach has been patched. These costs stem from losing the confidence of customers and industry observers. Damages to an organization's reputation are much harder to repair than a bypassed firewall.

Organizations must be prepared to evolve the methods they use to defend themselves against today's breed of hackers and cybercriminals. This includes incorporating best-of-breed technologies into their IT environments. Once deployed, these solutions must be maintained and tuned to make sure the protection level they provide remains consistent.

A best-of-breed approach isn't limited to just the technology. It also includes regular policy reviews, employee training, and achieving an organization-wide commitment to security. These elements are essential to guaranteeing the activities and attitudes of the organization and its partners continue to reflect the current threat arena.

Part IV: Who We Are

Arraya Solutions is a leading Mid-Atlantic technology consulting firm and managed services provider. Our customer base spans organizations of all sizes, representing a diverse collection of industries. We pride ourselves on our ability to deliver solutions that cover an array of today's biggest IT needs, including managed services, network and security, cloud, data center optimization, collaboration and communication, and mobility.

Since our founding in 1999, we have committed ourselves to the principle of combining the technological expertise common to large-scale providers with the close, personal service typically found in smaller IT partners. Our mission is to work with our customers, not for them, to develop and implement the best solutions to satisfy their particular business needs, objectives, and goals. In the process, we educate, engage, and empower IT departments and entire companies to succeed.

Part V: Methodology

The *2016 Cybersecurity Tactics Snapshot* was compiled using data collected at the 2016 Arraya Solutions Tech Summit. This yearly event brings together IT professionals from across the Mid-Atlantic region to learn about the latest solutions directly from our team of experts. Attendees of the Tech Summit were invited to fill out a brief survey on their cybersecurity environments in order to be entered into a prize drawing.

The following charts will provide a closer look at the demographics of those who completed the survey while keeping their identities and organization names anonymous.

Figure 8: Respondent Positions

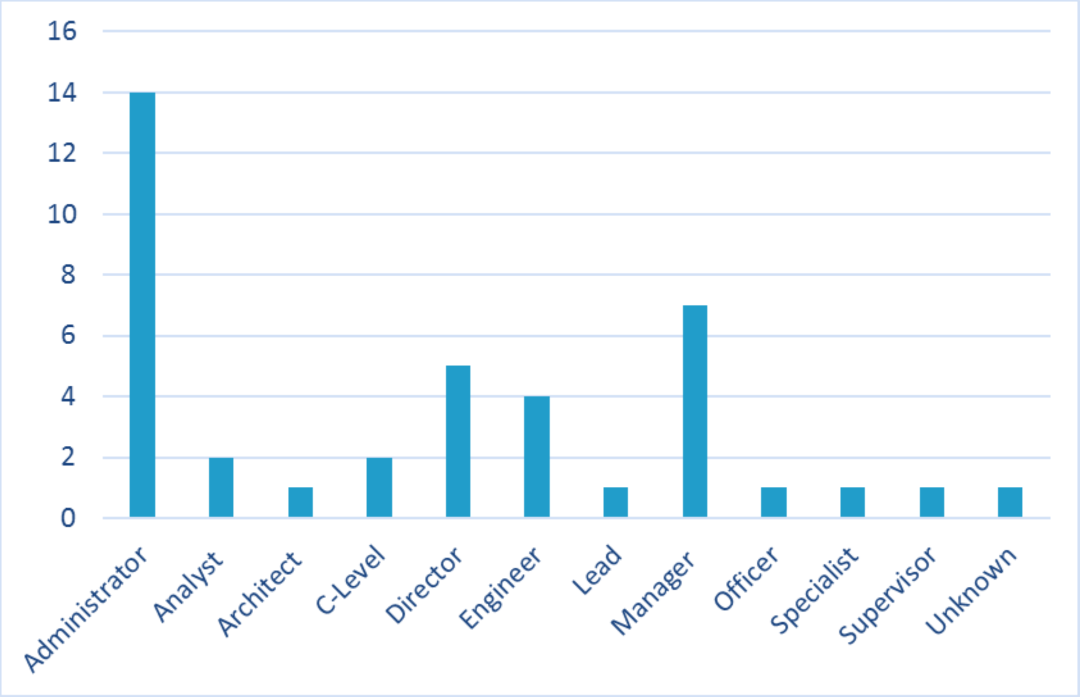
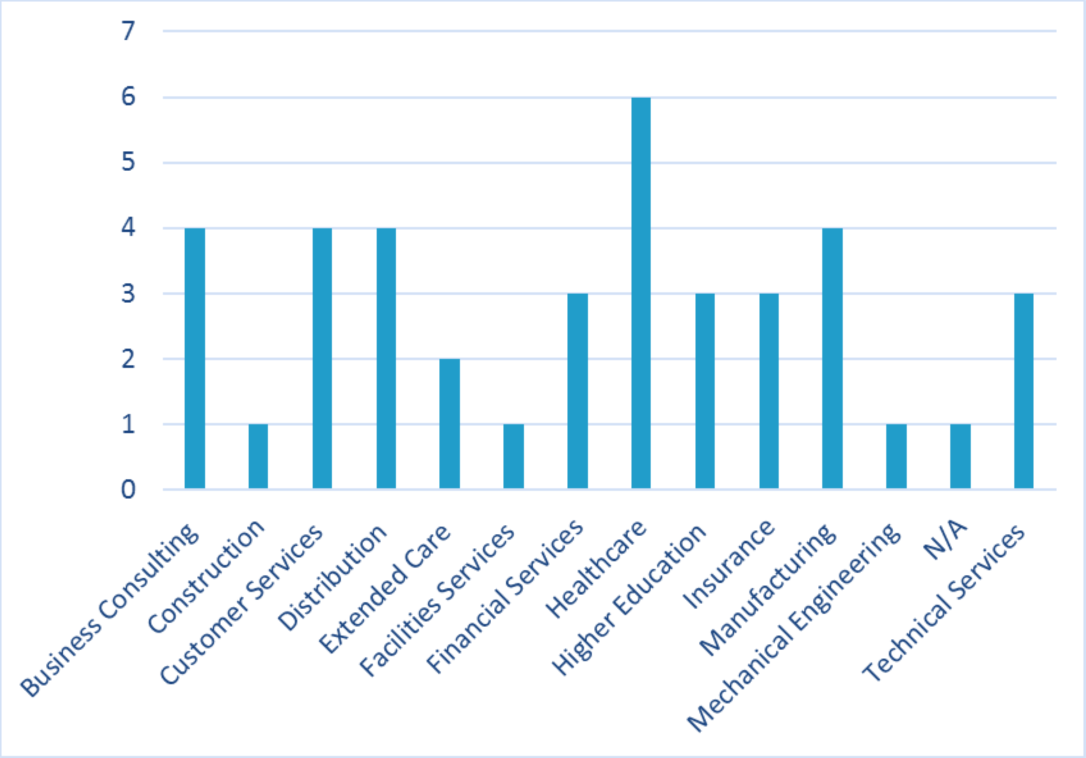


Figure 9: Industry Representation


Business Consulting
Construction
Customer Services
Distribution
Extended Care
Facilities Services
Financial Services
Healthcare
Higher Education
Insurance
Manufacturing
Mechanical Engineering
N/A
Technical Services