Flipping the Economics of Attacks

Sponsored by Palo Alto Networks

Independently conducted by Ponemon Institute LLC

Publication Date: January 2016

Flipping the Economics of Attacks

Ponemon Institute, January 2016

Part 1. Introduction

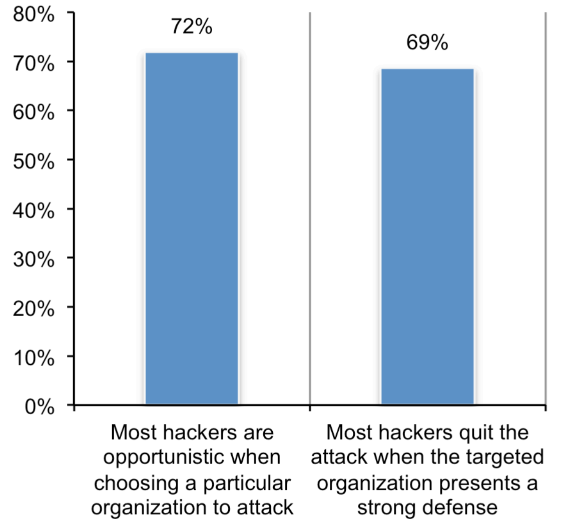
How much does it cost technically proficient adversaries to conduct successful attacks, and how much do they earn? In *Flipping the Economics of Attacks,* we look at the relationships between the time spent and compensation of today's adversaries and how organizations can thwart attacks. As revealed in this research, while some attackers may be motivated by non-pecuniary reasons, such as those that are geopolitical or reputational, an average of 69 percent of respondents say they are in it for the money.

In this study, we surveyed 304 threat experts in the United States, United Kingdom and Germany. We built this panel of experts based on their participation in Ponemon Institute activities and IT security conferences. They were assured their identity would remain anonymous. Twenty-one percent of respondents say they are very involved, and 79 percent of respondents are involved in the threat community. They are all familiar with present-day hacking methods.

Following are the most salient findings of this research:

Attackers are opportunistic. Adversaries go after the easiest targets first. As shown in Figure 1, they won't waste time on an attack that will not quickly result in a treasure trove of high-value information, according to 72 percent of respondents. Further, attackers will quit when the targeted company has a strong defense, according to 69 percent of respondents.

Figure 1. Attackers look for easy targets
Strongly agree and agree responses combined



Cost and time to plan and execute attacks is decreasing. According to 53 percent of respondents, the total cost of a successful attack has decreased, driving even more attacks across the industry. Similarly, 53 percent of respondents say the time to plan and execute an attack has decreased. Of these 53 percent of respondents who say it takes less time, 67 percent agree the number of known exploits and vulnerabilities has increased, 52 percent agree attacker skills have improved and 46 percent agree hacking tools have improved.

Increased usage of low-cost and effective toolkits drives attacks. Technically proficient attackers are spending an average of $1,367 for specialized toolkits to execute attack.[1] In the past two years, 63 percent of respondents say their use of hacker tools has increased and 64 percent of respondents say these tools are highly effective.

Time to deter the majority of attacks is less than two days. The longer an organization can keep the attacker from executing a successful attack the stronger its ability to safeguard its sensitive and confidential information. The inflection point for deterring the majority of attacks is less than two days (40 hours) resulting in more than 60 percent of all attackers moving on to another target.

[1] We assume that this average cost for specialized tools applies to all attacks launched over one year.

Adversaries make less than IT security professionals. On average, attackers earn $28,744 per year in annual compensation, which is about one-quarter of a cybersecurity professional's average yearly wage.

Organizations with strong defenses take adversaries more than double the time to plan and execute attacks. The average number of hours a technically proficient attacker takes to plan and execute an attack against an organization with a "typical" IT security infrastructure is less than three days (70 hours). However, when the company has an "excellent" IT infrastructure the time doubles to an average of slightly more than six days (147 hours).

Threat intelligence sharing is considered the most effective in preventing attacks. According to respondents, an average of 39 percent of all hacks can be thwarted because the targeted organization engaged in the sharing of threat intelligence with its peers.

Investments in security effectiveness can reduce successful attacks significantly. As an organization strengthens its security effectiveness, the ability to deter attacks increases, as shown in this report. The following are recommendations to harden organizations against malicious actors:

- Create a holistic approach to cyber security, which includes focusing on the three important components of a security program: people, process and technology.
- Implement training and awareness programs that educate employees on how to identify and protect their organization from such attacks as phishing.
- Build a strong security operations team with clear policies in place to respond effectively to security incidents.
- Leverage shared threat intelligence in order to identify and prevent attacks seen by your peers.
- Invest in next-generation technology such as threat intelligence sharing and integrated security platforms that can prevent attacks and other advanced security technologies.

Part 2. Key findings

In this section, we provide an analysis of the findings. The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics.

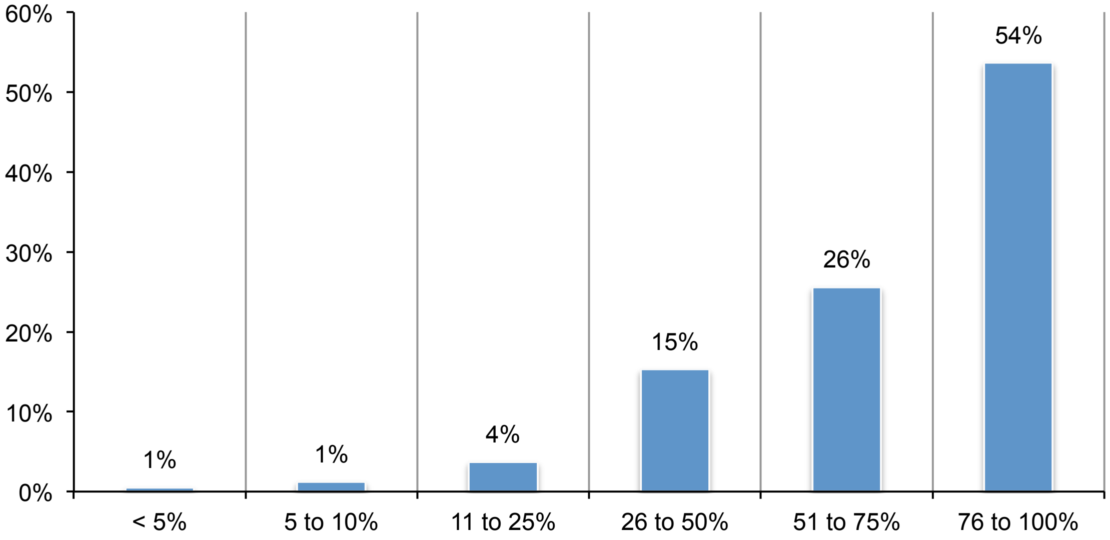
- The economic motivation of attackers
- Why successful attacks are increasing
- Inflection point: When malicious actors call it quits
- Hardening the organization against attackers

The economic motivation of attackers

What motivates an attacker? As shown in Figure 2, 69 percent of respondents in this study are motivated by money. While many attackers may be hoping for a big "payout", reality can be quite different. The findings reveal that attackers on average receive $28,744 for an average of 705 hours spent on attacks annually.

Of course, some attackers do "earn" more than the average. However, this compensation is 38.8 percent less than the average hourly rate of IT security practitioners employed in the private and public sector.

Figure 2. On average, what percent of attackers are motivated purely by economics (e.g., money) versus reputation or other non-pecuniary incentives?
Extrapolated average = 69 percent



Calculating the economics of hacking. To calculate the average adversary's compensation, we extrapolate the hours spent on attacks against organizations with a "typical" and "excellent" IT security infrastructure. As shown in Table 1, the time spent on an attack against an organization with an excellent IT security infrastructure is more than twice the time it takes when the organization has less than a strong security posture (e.g., 70 hours versus 147 hours per attack). The extrapolated pivot point where attackers would quit an attack is 209 hours on average.

From survey responses, we calculate an average value of $14,711 for each successful attack. We also calculate the average number of successful attacks per year at 8.26. The unadjusted economic gain per year equals $14,711 X 8.26. This value is adjusted by 42 percent (i.e. percent of successful attacks) and 59 percent (i.e. percent of successful attacks yielding a non-zero return). Finally, we reduce this adjusted value by the extrapolated cost of specialized tools of $1,367 used to improve the attacker's performance. The following is the basic equation, which yields an adjusted annual compensation of $28,744.

$28,744 = {[$14,711 X 8.26 X 42% X 59%] - $1,367}

Table 1. Economics of hacking

Calculus	Overall*
Hours spent on attack against typical IT security infrastructure	70
Hours spent on attack against excellent IT security infrastructure	147
Hours before quitting	209
Value per successful attack	$14,711
Number of attacks per year	8.26
Percent successful attacks	42.0%
Percent of successful attacks yielding non-zero return	59.0%
Cost of specialized tools	$1,367
Annual compensation	$28,744
Total hours spent per year	705
Labor rate per hour	$40.75
Rate per hour (benchmarks)	$60.36
Labor rate differential	$19.61
Percentage differential	38.8%

*Analysis conducted on the combined US, UK and German samples

To complete this analysis, we extrapolate the total hours that attackers devote to hacking activities each year. Drawing from prior research, we assume 80 percent of all attacks are lodged against organizations with a typical or ordinary security infrastructure and 20 percent with an excellent security infrastructure.[2] This yields a weighted average of 705 total hours per year. To derive an hourly attacker labor rate of $40.75, we simply divide adjusted annual compensation by total hours worked.

Does crime pay? For comparison purposes, we show an approximate labor rate derived from salary statistics compiled in recent research, where the fully loaded hourly labor rate for an experienced IT security professional is $60.36, which is 38.8 percent higher than the hourly rate compiled for attackers.[3] It is important to note attackers have more leisure time than gainfully employed security analysts. Our analysis assumes an average of only 705 hours worked per year for attackers versus 1,918 hours per annum by experienced IT security analysts.

[2] See: The Cyber Security Leap: From Laggard to Leader, Accenture & Ponemon Institute, April 2015

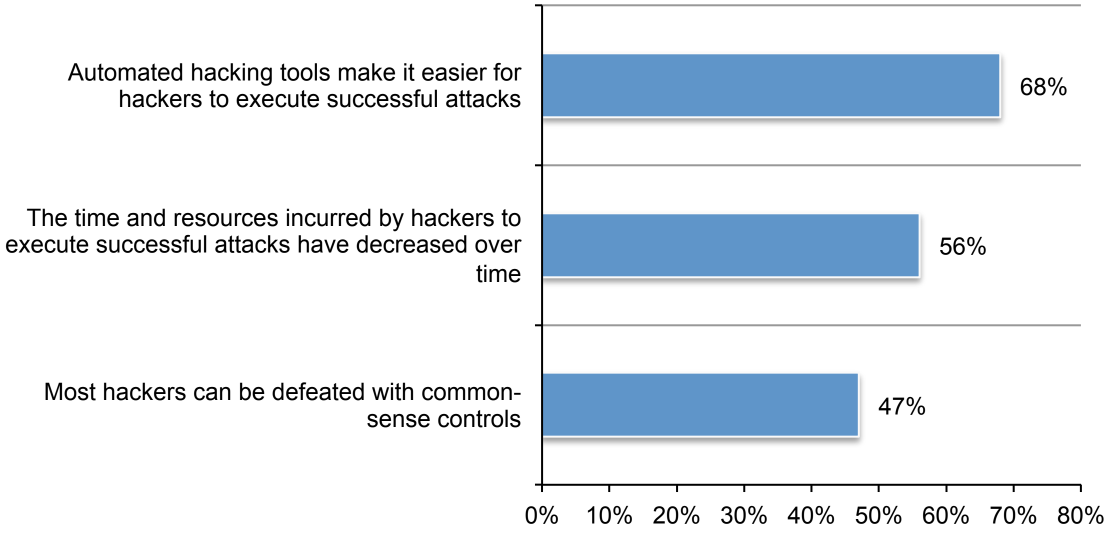
[3] See: Annual IT Security Benchmark Study. Ponemon Institute, July 2015.

Why successful attacks are increasing

Attacker technology is improving and makes more attacks possible. As shown in Figure 3, attackers are benefiting from automated hacking tools, which make it easier for attackers to execute a successful attack, according to 68 percent of respondents. Fifty-six percent of respondents say the time and resources incurred by attackers to execute a successful have decreased over time.

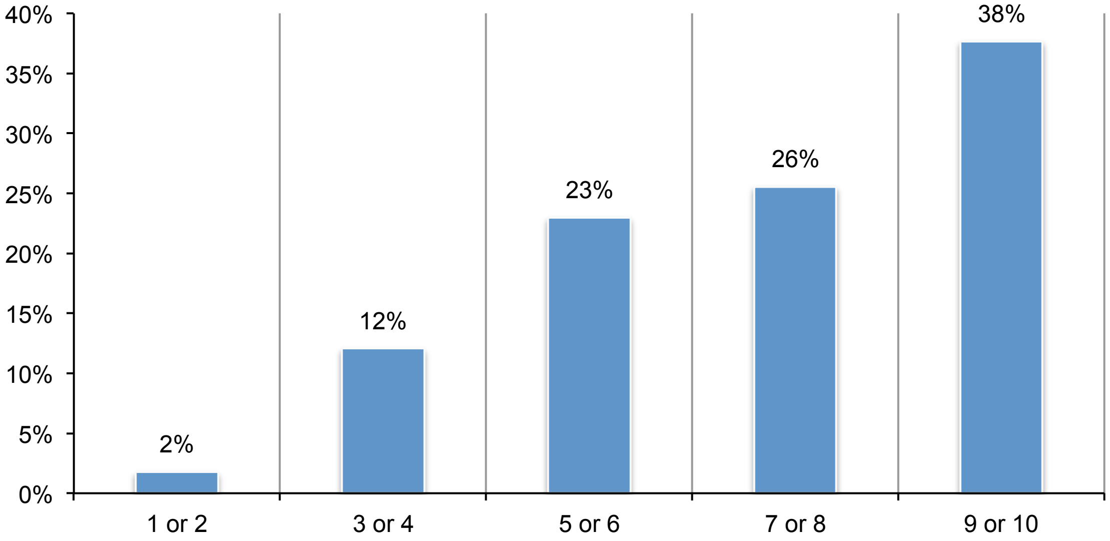
Expertise is not enough to defeat a motivated attacker. Only 47 percent of respondents say that common sense controls can stop a successful hack. To defeat attackers, organizations need to arm themselves with sophisticated technologies.

Figure 3. Why attacks are increasing
Strongly agree and agree responses combined



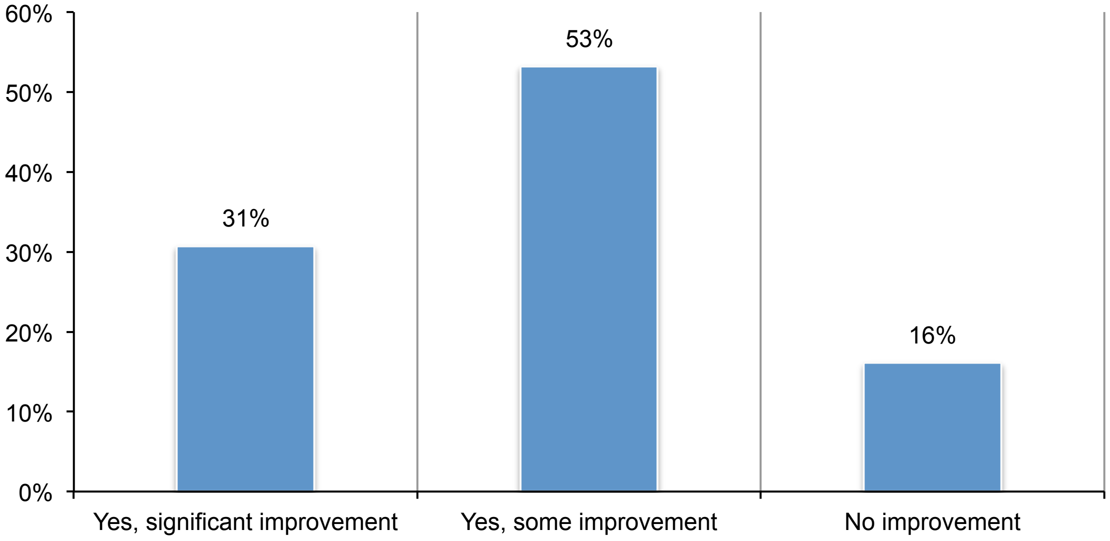
The cost of conducting successful attacks drops with the increasing use of hacker toolkits. Technically proficient adversaries are spending an average of $1,367 for specialized toolkits to execute attacks.[4] In the past two years, 63 percent of respondents say their use of hacker tools has increased by an average of 18 percent. Moreover, as shown in Figure 4, 64 percent of respondents (26+38) say these tools are highly effective.

Figure 4. How effective are hacker tools for exploiting targeted organizations?
7+ on a scale of 1=not effective to 10=highly effective



According to Figure 5, 84 percent of respondents either say there has been a significant improvement in hacker tools (31 percent) or there has been some improvement (53 percent). Only 16 percent of respondents say there has not been any improvement.

Figure 5. Hacker tools have improved and make it easier to execute a targeted attack
Consolidated view

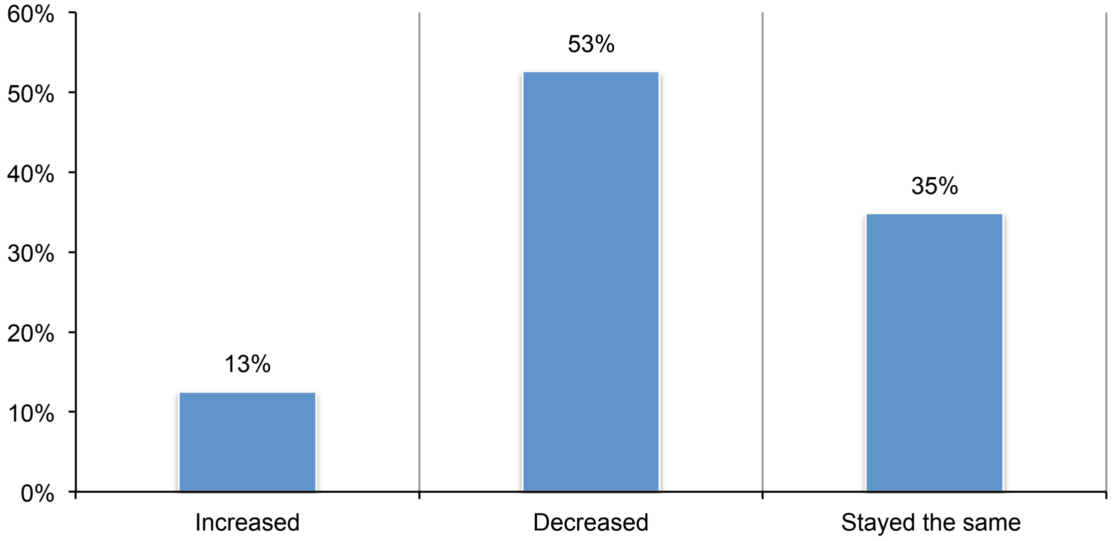


[4] Ibid Footnote 1

It costs less to hack**.** Not only are the hacker tools improving, the total cost of a successful attack has decreased, according to 53 percent of respondents, as shown in Figure 6. The reduction in cost is due to less time to execute a successful attack and in the improvement in hacker tools.

Contributing to the lower cost of a successful attack is the decrease in the cost of computing power. Cyber criminals can launch more sophisticated attacks for less investment. Today, bad actors without the capability to develop their own tools can use existing malware and exploits are often free or inexpensive to obtain online. Similarly, advanced attackers, criminal organizations and nation state attackers are able to use these widely available tools to launch successful intrusions and obscure their identities. These sophisticated adversaries are also developing and selectively using unique tools that could cause even greater harm.

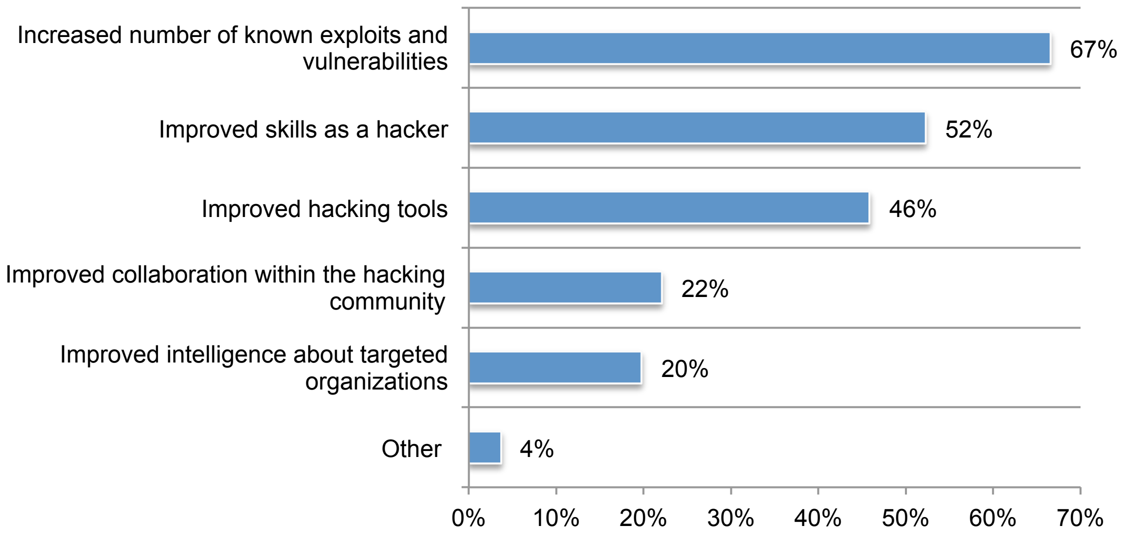
Figure 6. How has the total cost of a successful attack changed?
Consolidated view



Attackers are becoming more proficient. Eighty-five percent of respondents say the time to plan and execute an attack has either decreased (53 percent) or stayed the same (32 percent of respondents).

As shown in Figure 7 the primary reasons a decrease has occurred can be attributed to the increased number of known exploits and vulnerabilities (67 percent of respondents), improved skills as a hacker (52 percent of respondents) and improved hacking tools (46 percent of respondents).

Figure 7. Why the time to plan and execute an attack has decreased
More than one response permitted



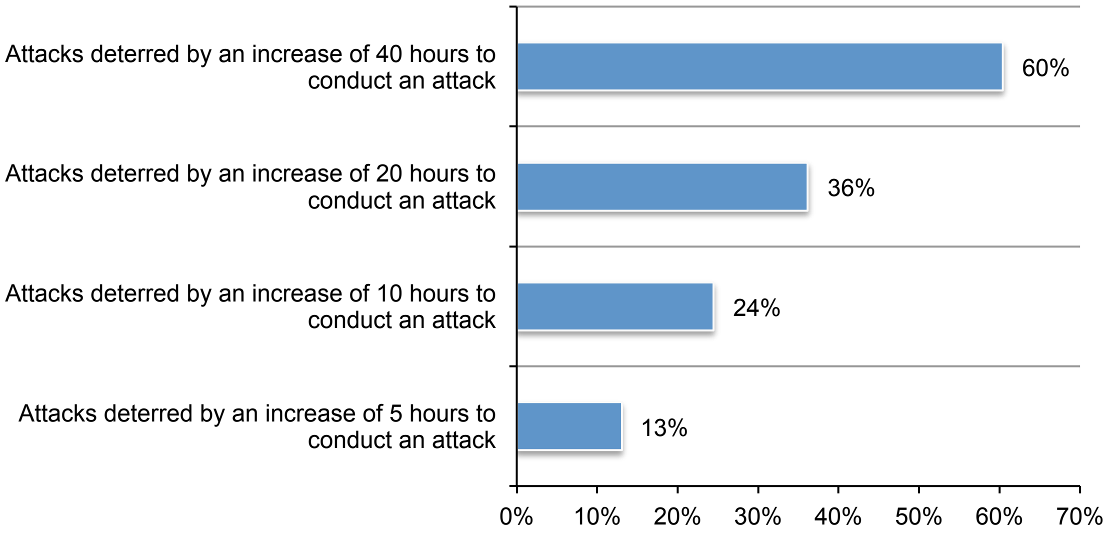
Inflection point: When malicious actors call it quits

Time to deter the majority of attacks is less than two days. We asked respondents how much time it takes to plan and execute web-based and malicious code attacks and if the time has increased, decreased or stayed the same. The study also examines how many of these attacks are successful and when does an attacker call it quits.

As shown in Figure 8, the longer an organization can keep the attacker from executing a successful attack, the stronger its ability to safeguard its sensitive and confidential information. While no organization has unlimited resources to spend hardening itself against malicious actors, understanding the amount of time until attackers' efforts are no longer potentially profitable will help the leadership prioritize investments in the appropriate technologies.

Time is the enemy of an attacker. The more time that passes before a successful attack can execute, the more likely an organization can stop it. For example, a delay of five hours in conducting a successful attack deters 13 percent of attacks, a delay of 10 hours can reduce 24 percent of attacks, and 20 hours deters 36 percent of attacks. On average, a technically proficient hacker will quit an attack and move to another target after spending less than nine days without success.

Figure 8. When will a hacker call it quits?
Consolidated view



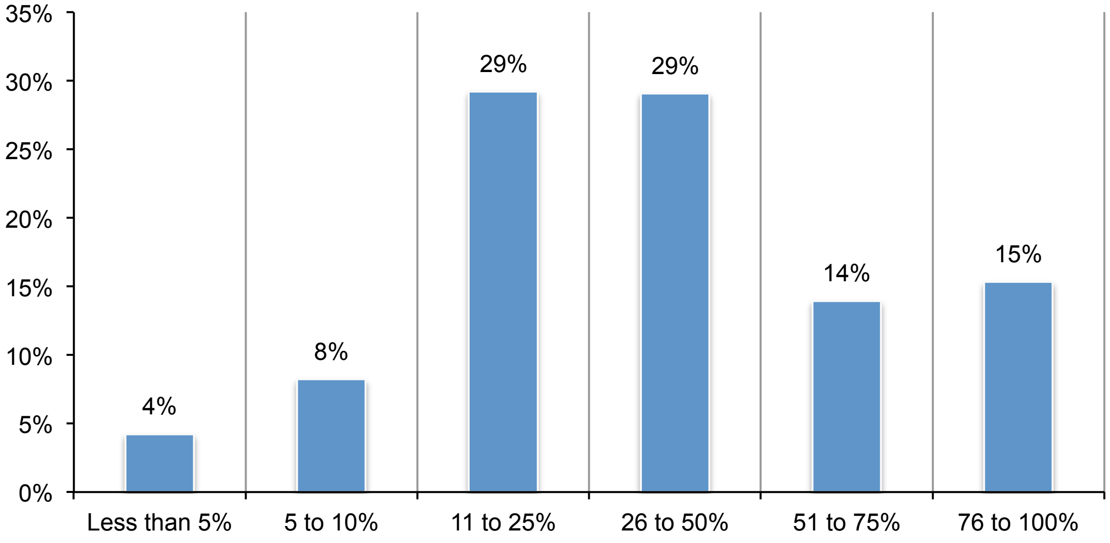
Malicious actors need to double the time to plan and execute successful attacks when the organization they target has an excellent IT infrastructure. In this study, we define an excellent IT security infrastructure as one that continually assesses threats, invests in leading-edge technologies and has adequate expertise supported by good governance practices. Whereas, the typical IT security infrastructure is less mature and may not deploy the technologies necessary to stop or curtail attackers. The following are other indications of an excellent IT security infrastructure:

- An advanced security system designed with definitive knowledge of what and who is using the network. In other words, no guessing.
- The capabilities of the advanced security system are integrated as much as possible into a platform so any suspicious action results in an automatic reprogramming of the other system's capabilities.
- The platform also must be part of a larger, global ecosystem that enables a constant and near real time sharing of attack information that can be used immediately to apply protections to prevent other organizations in the ecosystem from falling victim to the same or similar attacks.
- Where data resides or the network's deployment model should not affect security posture. For example, advanced integrated security and automated outcomes must be the same whether the network is on premise, in the cloud, or has data stored off the network in third party applications. Any inconsistency in the organization's security is a vulnerability point.
- Productivity should not be sacrificed because of security. Rather, security should be designed to support migration to the cloud, virtualization and other technologies that are important to the goals and objectives of the business.

Hardening the organization against attackers

Threat intelligence sharing is considered most effective in preventing attacks. To make it more difficult to execute a successful attack, the solution is to exchange threat intelligence with peers and to invest in the appropriate technologies to strengthen an organization's security posture. As shown in Figure 10, an average of 39 percent of all hacks can be thwarted because the targeted organization engaged in the sharing of threat intelligence with its peers. Additionally, out of all technologies available, threat intelligence sharing was cited by 55 percent of respondents as the most likely to prevent or curtail successful attacks.

Figure 10. What percent of all hacks can be thwarted because of threat intelligence sharing with peers?
Extrapolated average = 39 percent



Conclusion and recommendations

It is clear the attack landscape has changed. Each day we see more successful data breaches against organizations around the globe. This study has exposed as important element of this criminal underground, which can often be missed when headlines about the next big data breach dominate the front page: the economic motivation of cybercriminals and how we can use this information to turn the tables on them. The findings clearly show the profit-based motivation of attackers, which means the same economic forces are at work for them as for major businesses. Adversaries are in it for the quick and easy payday, with the majority of them making far less than comparable IT security professionals.

We expect the cost of attacks to continue to decrease, as attackers become more skilled and automated toolkits are improved and in widespread use, as well as other factors examined in this survey. There is another side to the cost equation though, which the security community can use to keep it safe. We can change the economics of attacks, by putting up a better defense, which takes attackers much longer to overcome.

This survey has shown how attackers will divert their attention to other targets after an increase in the time it takes to breach an organization of less than two days. Like many businesses, adversaries are constantly weighing the potential profit versus cost, which includes the time it takes them to be successful. As a security community, we must take into account the motivation and economic environment surround attacks, not just technical solutions to the problem. In order to increase the cost to the attacker, we recommend organizations take the following action to enhance their security:

- Create a holistic approach to cyber security, which includes focusing on the three important components of a security program: people, process and technology.
- Implement training and awareness programs that educate employees on how to identify and protect their organization from such attacks as phishing.
- Build a strong security operations team with clear policies in place to respond effectively to security incidents.
- Invest in next-generation technology, such as threat intelligence sharing and integrated security platforms, that can prevent attacks, and other advanced security technologies.

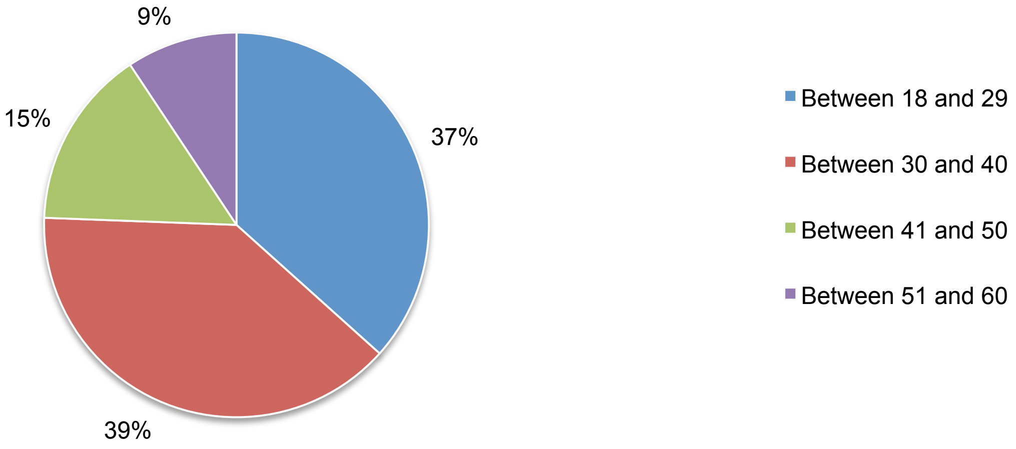
Part 3. Methods

A sampling frame of 10,332 individuals with self-proclaimed hacking skills located in the United States, United Kingdom and Germany were selected as participants to this survey. Table 1 shows 379 total returns. Post screening and reliability checks required the removal of 75 surveys. Our final sample consisted of 304 surveys or a 2.9 percent response rate.

Table 2. Sample response	US	UK	DE	Combined
Sampling frame	5,055	2,632	2,645	10,332
Total returns	197	89	93	379
Post-screened and rejected surveys	39	19	17	75
Final sample	158	70	76	304
Response rate	3.1%	2.7%	2.9%	2.9%

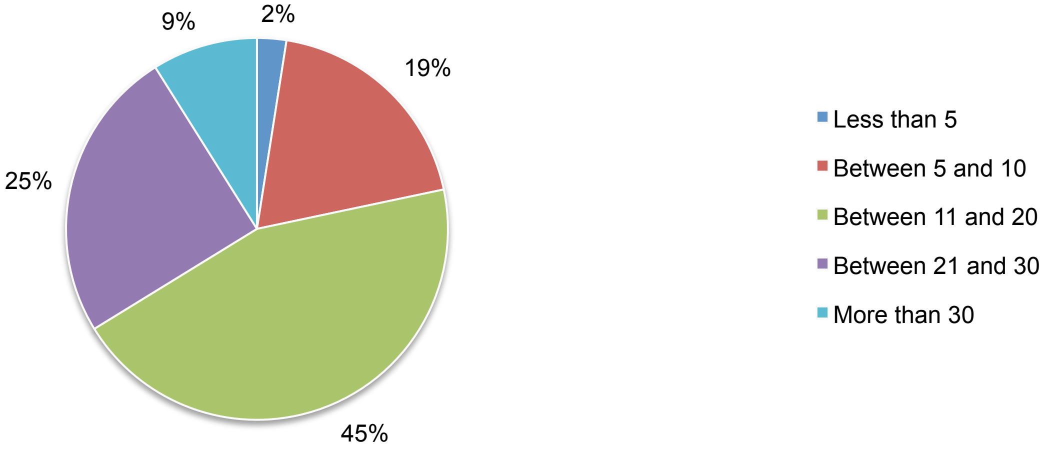
Pie Chart 1 reports the respondent's age. Thirty-seven percent of respondents are between the ages of 18 and 29 and 39 percent are between 30 and 40 years of age.

Pie Chart 1. Respondent's age range



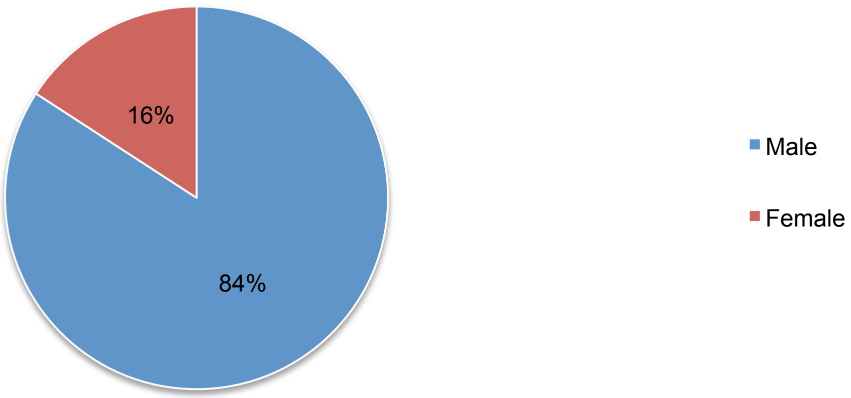
As shown in Pie Chart 2, 19 percent of respondents have between 5 and 10 years of experience and almost half (45 percent) of respondents have between 11 and 20 years of experience.

Pie Chart 2. Years of experience in hacking and/or IT security activities such as penetration testing



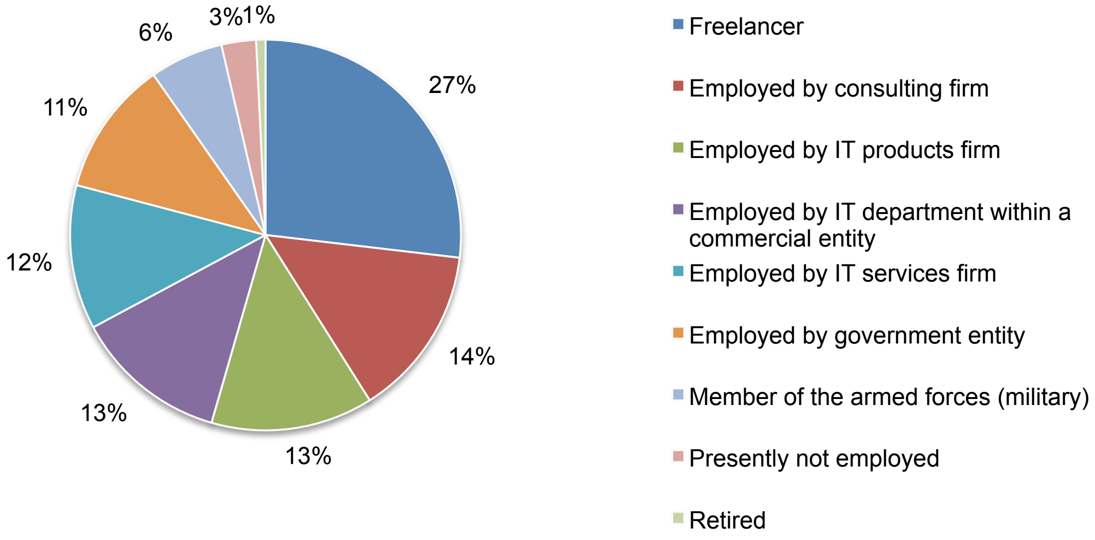
Eighty-four percent of respondents are male and 16 percent are female.

Pie Chart 3. Gender



As shown in Pie Chart 4, 27 percent of respondents reported their employment status as freelancer, 14 percent are employed by a consulting firm and 13 percent are employed by IT products firm and another 23 percent are employed by IT department within a commercial entity.

Pie Chart 4. Employment status



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are white and black hat attackers located in the United States, United Kingdom and Germany. We also acknowledge that the results may be biased by external events, such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2015.

Survey response	US	UK	DE	Combined
Sampling frame	24,556	16,501	17,095	58,152
Pre-screened	19,501	13,869	14,450	47,820
Adjusted sampling frame	5,055	2,632	2,645	10,332
Total returns	197	89	93	379
Post-screened and rejected surveys	39	19	17	75
Final sample	158	70	76	304
Response rate	3.1%	2.7%	2.9%	2.9%
Sample weighting	0.52	0.23	0.25	1.00

Screening questions

S1. What best describes your level of familiarity with present-day hacking methods?	US	UK	DE	Combined
Very familiar	56%	50%	64%	57%
Familiar	44%	50%	36%	43%
Not familiar (stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

S2. What best describes your level of experience in successfully penetrating computer systems (as a black hat and/or white hat)?	US	UK	DE	Combined
Very experienced	66%	61%	71%	66%
Experienced	34%	39%	29%	34%
Not experienced (stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

S3. What best describes your level of involvement in the hacker community?	US	UK	DE	Combined
Very involved	20%	23%	21%	21%
Involved	80%	77%	79%	79%
Not involved (stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

Q1a. On average, how much time does it take a technically proficient hacker to plan and execute an **attack** against an organization with a "typical" IT security infrastructure?	US	UK	DE	Combined
1 to 60 minutes	6%	6%	7%	6%
1 to 24 hours	52%	54%	57%	53%
1 to 7 days	32%	26%	22%	28%
1 to 4 weeks	12%	15%	15%	13%
1 to 12 months	0%	0%	0%	0%
More than 1 year	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value (hours)	67	76	72	70

Q1b. Looking back over the past 2 years, has the time to plan and execute an attack increased, decreased or stayed the same?	US	UK	DE	Combined
Increased	16%	15%	13%	15%
Decreased	55%	50%	51%	53%
Stayed the same	29%	35%	36%	32%
Total	100%	100%	100%	100%

Q1c. If you selected decreased, why?	US	UK	DE	Combined
Improved skills as a hacker	53%	52%	51%	52%
Improved collaboration within the hacking community	25%	21%	17%	22%
Improved intelligence about targeted organizations	20%	19%	22%	20%
Improved hacking tools	44%	45%	51%	46%
Increased number of known exploits and vulnerabilities	69%	60%	68%	67%
Other (please specify)	4%	5%	4%	4%
Total	214%	201%	212%	210%

Q2a. On average, how much time does it take a technically proficient hacker to plan and execute an attack against an organization with an "excellent" IT security infrastructure?	US	UK	DE	Combined
1 to 60 minutes	2%	2%	3%	2%
1 to 24 hours	45%	40%	40%	42%
1 to 7 days	34%	38%	35%	35%
1 to 4 weeks	18%	19%	22%	20%
1 to 12 months	2%	1%	1%	1%
More than 1 year	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value (hours)	159	143	130	147

Q2b. Based on your experience, what percent of all attacks executed by technically proficient attacker are successful (i.e., not stopped by firewalls and other perimeter controls)? Assume the targeted organization had a typical IT security infrastructure.	US	UK	DE	Combined
Less than 5%	2%	4%	2%	2%
5 to 10%	14%	14%	9%	13%
11 to 25%	23%	24%	18%	22%
26 to 50%	24%	21%	25%	23%
51 to 75%	25%	25%	31%	26%
76 to 100%	13%	13%	16%	13%
Total	100%	100%	100%	100%
Extrapolated value	40%	40%	46%	42%

Q2c. On average, how much time does a technically proficient hacker take before he or she quits an attack and moves to another target?	US	UK	DE	Combined
1 to 60 minutes	0%	0%	0%	0%
1 to 24 hours	13%	17%	13%	14%
1 to 7 days	48%	52%	53%	51%
1 to 4 weeks	38%	30%	34%	34%
1 to 12 months	1%	2%	1%	1%
More than 1 year	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value (hours)	213	211	203	209

Q3a. Approximately, how much money is earned as a result of one successful attack by a technically proficient hacker? Earnings include cash, virtual currencies and other forms of compensation. For comparison purposes, the UK and German survey ranges were converted from local currency (e.g., GBP and Euro) to the U.S. dollar.	US	UK	DE	Combined
Less than $500	2%	4%	0%	2%
500 to $1,000	10%	7%	11%	10%
1,001 to $5,000	16%	16%	15%	16%
5,001 to $10,000	21%	32%	23%	24%
10,001 to $25,000	36%	30%	38%	35%
25,001 to $50,000	12%	11%	11%	12%
50,001 to $100,000	2%	0%	1%	1%
More than $100,000	1%	0%	1%	1%
Total	100%	100%	100%	100%
Extrapolated value (US$ Dollars)	$15,638	$12,324	$14,983	$14,711

Q3b. Approximately, what percentage of successful attacks do not yield any compensation?	US	UK	DE	Combined
Less than 5%	0%	2%	0%	0%
5 to 10%	0%	1%	5%	1%
11 to 25%	24%	28%	35%	28%
26 to 50%	50%	43%	35%	45%
51 to 75%	12%	13%	17%	13%
76 to 100%	14%	13%	8%	12%
Total	100%	100%	100%	100%
Extrapolated value	43%	41%	37%	41%

Q4. On average, how many successful attacks are executed each year by a technically proficient hacker?	US	UK	DE	Combined
1 (One)	2%	2%	0%	2%
2 to 5	25%	31%	28%	27%
6 to 10	49%	44%	45%	47%
11 to 15	20%	21%	21%	20%
16 to 25	3%	2%	5%	3%
More than 25	1%	0%	1%	1%
Total	100%	100%	100%	100%
Extrapolated value	8.32	7.76	8.61	8.26

Q5. Approximately, how much do technically proficient attacker spend on specialized tools (e.g., hacker tool kits) to execute attacks? For comparison purposes, the UK and German survey ranges were converted from local currency (e.g., GBP and Euro) to the U.S. dollar.	US	UK	DE	Combined
Less than $100	22%	23%	25%	23%
100 to $500	24%	26%	28%	25%
501 to $1,000	33%	26%	25%	29%
1,001 to $2,500	7%	9%	11%	8%
2,501 to $5,000	8%	11%	7%	8%
5,001 to $10,000	3%	4%	2%	3%
10,001 to $25,000	2%	1%	2%	2%
More than $25,000	1%	0%	0%	1%
Total	100%	100%	100%	100%
Extrapolated value (US$ Dollars)	$1,557	$1,229	$1,179	$1,367

Q6. Using the following 10-point scale, please rate the effectiveness of hacker tools for exploiting targeted organizations. 1 = not effective to 10 = highly effective.	US	UK	DE	Combined
1 or 2	1%	0%	5%	2%
3 or 4	11%	8%	18%	12%
5 or 6	20%	22%	30%	23%
7 or 8	29%	26%	18%	26%
9 or 10	39%	44%	29%	38%
Total	100%	100%	100%	100%
Extrapolated value	7.38	7.62	6.46	7.21

Q7. Over time have hacker tools improved, thereby making it easier to execute a targeted attack?	US	UK	DE	Combined
Yes, significant improvement	31%	33%	28%	31%
Yes, some improvement	56%	46%	54%	53%
No improvement	13%	21%	18%	16%
Totals	100%	100%	100%	100%

Q8a. Over the past 24 months, how has the use of hacker tools changed?	US	UK	DE	Combined
Increased	65%	62%	59%	63%
Decreased	12%	15%	10%	12%
Stayed the same (skip Q9)	23%	23%	31%	25%
Total	100%	100%	100%	100%

Q9. If increased, by how much?	US	UK	DE	Combined
< 2%	0%	2%	6%	2%
2 to 5%	3%	6%	7%	5%
6 to 10%	12%	11%	14%	12%
11 to 15%	21%	20%	18%	20%
16 to 20%	30%	32%	29%	30%
21 to 30%	18%	21%	23%	20%
31 to 40%	8%	6%	3%	6%
41 to 50%	8%	2%	0%	5%
More than 50%	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value	20%	18%	16%	18%

Q10. Over the past 24 months, how has the total cost of a successful attack changed? Cost include the value of time and tools used to unleash attacks.	US	UK	DE	Combined
Increased	14%	12%	10%	13%
Decreased	56%	50%	48%	53%
Stayed the same (skip Q11)	30%	38%	42%	35%
Total	100%	100%	100%	100%

Q11. If decreased, by how much?	US	UK	DE	Combined
< 2%	0%	1%	2%	1%
2 to 5%	5%	5%	4%	5%
6 to 10%	10%	7%	10%	9%
11 to 15%	19%	23%	22%	21%
16 to 20%	23%	26%	20%	23%
21 to 30%	11%	12%	14%	12%
31 to 40%	8%	6%	3%	6%
41 to 50%	8%	7%	11%	9%
More than 50%	16%	13%	14%	15%
Total	100%	100%	100%	100%
Extrapolated value	26%	24%	25%	25%

Q12. On average, what percent of attacker are motivated purely by economics (e.g., money) versus reputation or other non-pecuniary incentives?	US	UK	DE	Combined
Less than 5%	0%	0%	2%	1%
5 to 10%	0%	1%	4%	1%
11 to 25%	2%	3%	8%	4%
26 to 50%	16%	14%	15%	15%
51 to 75%	22%	43%	17%	26%
76 to 100%	60%	39%	54%	54%
Total	100%	100%	100%	100%
Extrapolated value	73%	67%	65%	69%

Q13. In your opinion, what percent of all hacks can be thwarted because the targeted organization engaged in the sharing of threat intelligence with their peers?	US	UK	DE	Combined
Less than 5%	5%	6%	1%	4%
5 to 10%	10%	11%	2%	8%
11 to 25%	29%	31%	28%	29%
26 to 50%	28%	25%	35%	29%
51 to 75%	12%	15%	17%	14%
76 to 100%	16%	12%	17%	15%
Total	100%	100%	100%	100%
Extrapolated value	38%	36%	44%	39%

Q14a. An increase of 5 **hours** in the time it takes to conduct a successful attack will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	36%	40%	30%	35%
5 to 10% of attacks	33%	31%	29%	32%
11 to 25% of attacks	19%	16%	28%	21%
26 to 50% of attacks	10%	8%	7%	9%
51 to 75% of attacks	2%	5%	5%	3%
76 to 100% of attacks	0%	0%	1%	0%
Total	100%	100%	100%	100%
Extrapolated value	12%	13%	15%	13%

Q14b. An increase of 10 **hours** in the time it takes to conduct a successful attack will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	21%	29%	21%	23%
5 to 10% of attacks	32%	28%	28%	30%
11 to 25% of attacks	17%	15%	25%	19%
26 to 50% of attacks	11%	10%	14%	12%
51 to 75% of attacks	4%	5%	6%	5%
76 to 100% of attacks	15%	13%	6%	12%
Total	100%	100%	100%	100%
Extrapolated value	26%	24%	22%	24%

Q14c. An increase of 20 **hours** in the time it takes to conduct a successful attack will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	6%	8%	6%	6%
5 to 10% of attacks	12%	10%	9%	11%
11 to 25% of attacks	21%	28%	24%	23%
26 to 50% of attacks	35%	29%	34%	33%
51 to 75% of attacks	16%	15%	21%	17%
76 to 100% of attacks	10%	10%	6%	9%
Total	100%	100%	100%	100%
Extrapolated value	37%	35%	36%	36%

Q14d. An increase of 40 **hours** in the time it takes to conduct a successful attack will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	0%	0%	0%	0%
5 to 10% of attacks	3%	0%	1%	2%
11 to 25% of attacks	11%	8%	10%	10%
26 to 50% of attacks	23%	18%	26%	23%
51 to 75% of attacks	26%	32%	34%	29%
76 to 100% of attacks	37%	42%	29%	36%
Total	100%	100%	100%	100%
Extrapolated value	59%	65%	58%	60%

For questions Q15a to Q15d, please assume a security effectiveness scale from 1 = very poor security posture to 10 = very strong security posture.				
Q15a. An increase of 2 points on a 10-point scale (from 2 to 4) will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	25%	26%	32%	27%
5 to 10% of attacks	29%	28%	25%	28%
11 to 25% of attacks	19%	17%	21%	19%
26 to 50% of attacks	19%	11%	12%	15%
51 to 75% of attacks	2%	9%	6%	5%
76 to 100% of attacks	6%	9%	4%	6%
Total	100%	100%	100%	100%
Extrapolated value	20%	24%	19%	21%

Q15b. An increase of 4 points on a 10-point scale (from 2 to 6) will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	15%	16%	15%	15%
5 to 10% of attacks	26%	28%	24%	26%
11 to 25% of attacks	19%	17%	21%	19%
26 to 50% of attacks	13%	12%	17%	14%
51 to 75% of attacks	15%	14%	13%	14%
76 to 100% of attacks	12%	13%	10%	12%
Total	100%	100%	100%	100%
Extrapolated value	31%	30%	29%	30%

Q15c. An increase of 6 points on a 10-point scale (from 2 to 8) will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	5%	4%	3%	4%
5 to 10% of attacks	10%	8%	4%	8%
11 to 25% of attacks	12%	16%	15%	14%
26 to 50% of attacks	26%	28%	27%	27%
51 to 75% of attacks	19%	23%	27%	22%
76 to 100% of attacks	28%	21%	24%	25%
Total	100%	100%	100%	100%
Extrapolated value	49%	47%	51%	49%

Q15d. An increase of 8 points on a 10-point scale (from 2 to 10) will deter . . . (choose one)	US	UK	DE	Combined
Less than 5% of attacks	0%	0%	0%	0%
5 to 10% of attacks	0%	0%	0%	0%
11 to 25% of attacks	15%	12%	8%	13%
26 to 50% of attacks	16%	18%	12%	15%
51 to 75% of attacks	19%	16%	23%	19%
76 to 100% of attacks	50%	54%	57%	53%
Total	100%	100%	100%	100%
Extrapolated value	64%	66%	70%	66%

Q16. Which of the following enabling security technologies are most likely to stop or curtail attacker from executing successful attacks. Please choose your **top five (5)** technologies.	US	UK	DE	Combined
Threat intelligence sharing	55%	52%	57%	55%
Identity management & authentication	45%	54%	49%	48%
Security information and event management (SIEM)	44%	42%	46%	44%
Next generation firewalls and UTMs	38%	37%	45%	40%
Network and traffic intelligence systems	34%	35%	41%	36%
Hack back solutions	34%	35%	30%	33%
Honeypot solutions	33%	31%	35%	33%
Encryption for data at rest	28%	28%	32%	29%
Intrusion detection (IDS) and/or prevention (IPS)	23%	24%	25%	24%
Endpoint security solutions	20%	24%	27%	23%
Encryption for data in motion	22%	19%	24%	22%
Web application firewalls (WAF)	16%	10%	22%	16%
Virtual private networks (VPN)	11%	18%	16%	14%
Multi-layered firewall defense	20%	13%	1%	14%
Data loss prevention (DLP)	18%	17%	1%	14%
Sandboxing solutions	15%	12%	11%	13%
Code review and debugging systems	12%	7%	8%	10%
Access governance	8%	18%	6%	10%
Anti-virus & anti-malware	9%	13%	8%	10%
Big data analytics	8%	6%	8%	8%
Wireless security solutions	7%	5%	8%	7%
Total	500%	500%	500%	500%

Part 4: Attributions. Please rate the following seven statements using the scale provided below each item. Strongly agree and Agree responses combined.	US	UK	DE	Combined
Q17a. Most black hat attacker can earn more income serving business and government as a white hat.	68%	61%	59%	64%
Q17b. Most attacker are opportunistic when choosing a particular organization to attack.	73%	75%	67%	72%
Q17c. Automated hacking tools makes it easier for attacker to execute successful attacks.	70%	69%	64%	68%
Q17d. Most attacker quit the attack when the targeted organization presents a strong defense.	72%	66%	64%	69%
Q17e. Most attacker can be defeated with common-sense controls.	49%	45%	46%	47%
Q17f. The community of attacker has grown over time.	51%	55%	50%	52%
Q17g. The time and resources incurred by attacker to execute successful attacks have decreased over time.	59%	62%	44%	56%

D1. What best describes your age range?	US	UK	DE	Combined
Between 18 and 29	38%	35%	35%	37%
Between 30 and 40	36%	44%	40%	39%
Between 41 and 50	15%	13%	17%	15%
Between 51 and 60	11%	8%	7%	9%
More than 60	0%	0%	1%	0%
Total	100%	100%	100%	100%

D2. What best describes your years of experience in hacking and/or IT security activities such as penetration testing?	US	UK	DE	Combined
Less than 5	2%	3%	3%	2%
Between 5 and 10	19%	21%	18%	19%
Between 11 and 20	45%	43%	45%	45%
Between 21 and 30	26%	22%	25%	25%
More than 30	8%	11%	9%	9%
Total	100%	100%	100%	100%

D3. Gender?	US	UK	DE	Combined
Male	81%	85%	90%	84%
Female	19%	15%	10%	16%
Total	100%	100%	100%	100%

D4. Employment status?	US	UK	DE	Combined
Freelancer	23%	30%	32%	27%
Employed by IT services firm	10%	13%	15%	12%
Employed by IT products firm	17%	9%	10%	13%
Employed by consulting firm	13%	16%	15%	14%
Employed by IT department within a commercial entity	11%	13%	16%	13%
Employed by government entity	16%	7%	5%	11%
Member of the armed forces (military)	9%	5%	1%	6%
Presently not employed	0%	7%	5%	3%
Retired	1%	0%	1%	1%
Other	0%	0%	0%	0%
Total	100%	100%	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.