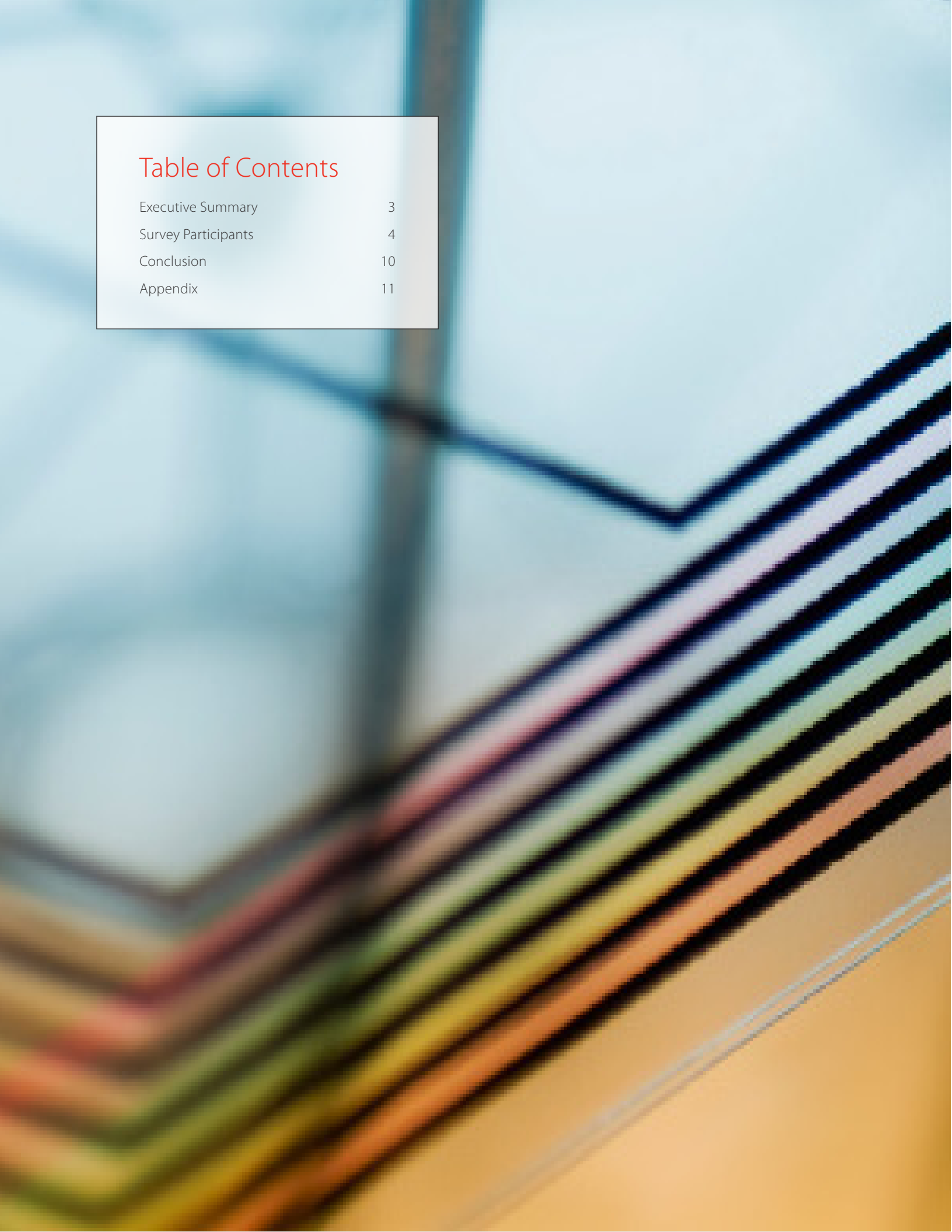
2012 Bit9 Cyber Security Research Report

Bit9

Table of Contents

Executive Summary	3
Survey Participants	4
Conclusion	10
Appendix	11



Executive Summary

According to the results of a recent survey conducted by Bit9, IT and security professionals are well aware of the changing nature of cyber attacks; how advanced attacks target their infrastructure; and what they would like to see as the most effective strategies for protecting their organizations. Importantly, the majority of IT and security professionals believe their organizations will be the target of an advanced attack within the next six months—and that this is neither due to lax security nor "media hype." In addition:

IT and security professionals (61%) feel that attacks will most likely come from Anonymous/hacktivists, cyber criminals and nation states in the next six months. Skilled, organized and well-funded attacks by these groups represent advanced threats to business critical information and intellectual property (IP). Advanced attacks are characterized by careful planning, manipulation by remote operators—and patience.

Anonymous/hacktivists are identified by 61% of the respondents as the most likely group to attack companies in the next six months.

The most anticipated method of cyber attack, by almost half the respondents is malware, e.g. Trojans, rootkits, worms, viruses, etc.

Most respondents do not feel their current cyber security is highly effective in protecting their most important and vulnerable machines: infrastructure servers.

74% of respondents feel the security of their endpoints – their laptops and desktops – is ineffective. Only 26% feel their current endpoint security solutions are doing a good job. As a result, endpoints are considered the most at risk.

The majority believe that the implementation of best practices and better security policies will have the biggest impact on improving cyber security against advanced threats. Despite all of the cyber security legislation, IT and security professionals do not have faith in regulated solutions; only 7% cited governmental legislation as having any impact on improving security.

This last finding has significant implications for enterprise cyber security postures: To be most effective, security solutions must follow best practices specific to combating the unique characteristics of advanced threats as well as reflect the security policies of each individual enterprise.

Survey Participants

In March and April of 2012, Bit9 conducted an online survey of 1,861 IT and security professionals worldwide. Survey participants work in companies across a wide range of industries, as well as in government agencies. The majority of the respondents (66%) work in organizations with more than 500 employees.

KEY SURVEY FINDINGS

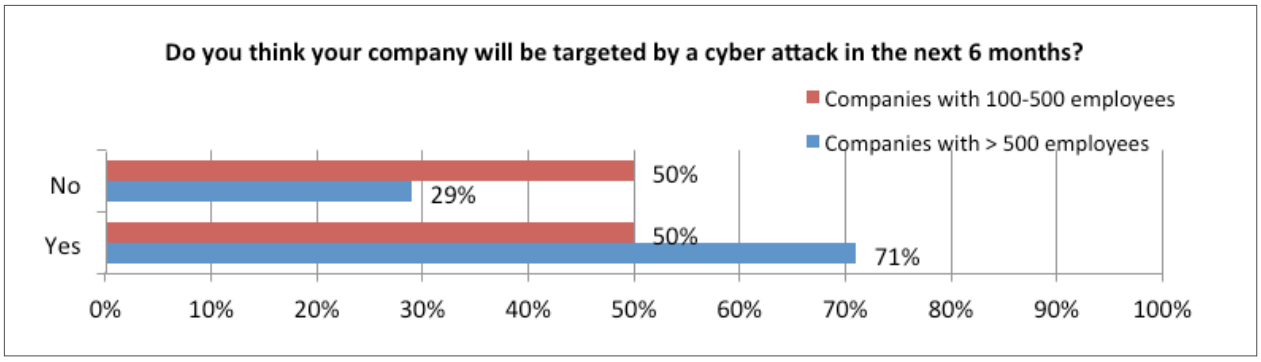
Key Finding #1: Most IT/Security professionals are well aware of the growing sophistication of cyber threats and the types of attackers they face.

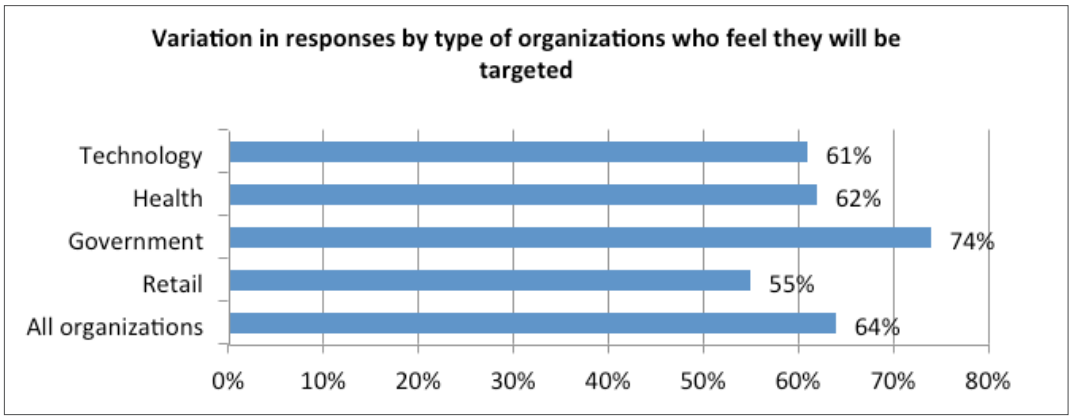
Nearly two-thirds of those surveyed feel their companies will be targeted by a cyber attack in the next six months. Professionals working in larger organizations (more than 500 employees) are significantly more concerned than those in companies of 100-500 workers.

Over half of the respondents in every market segment surveyed feel they will be targeted by a cyber attack in the next six months, though there were some significant differences in a few key segments. Perhaps understandably, government security professionals feel they are most likely to be attacked (74%) compared to a significantly smaller percentage (though still a majority) of respondents in the retail industry (55%).

This is consistent with a 2010 study conducted by the Ponemon Institute. The Ponemon Institute study found that "83 percent of respondents believe their organization has been the target of an advanced threat; 71 percent believe they have seen an increase in advanced threats over the past 12 months."

Two-thirds of the study participants believe the increase in cyber attacks is neither due to "media hype" nor perceived weaknesses in their defenses, but rather the result of a growing number of hackers, as well as better organized criminal groups and nation state perpetrators.

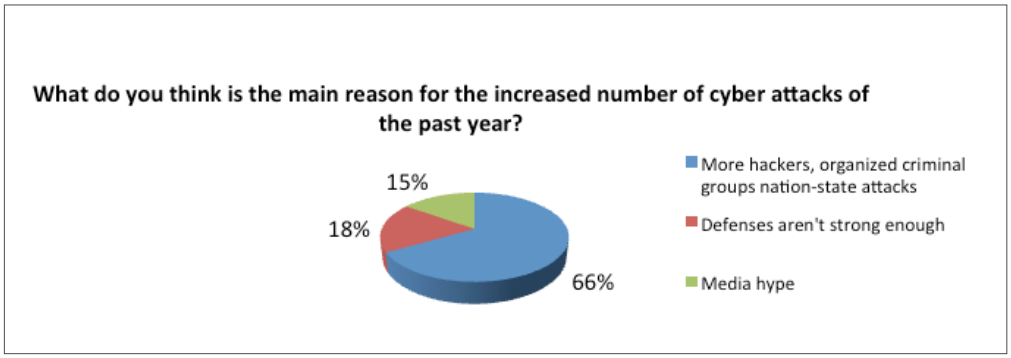


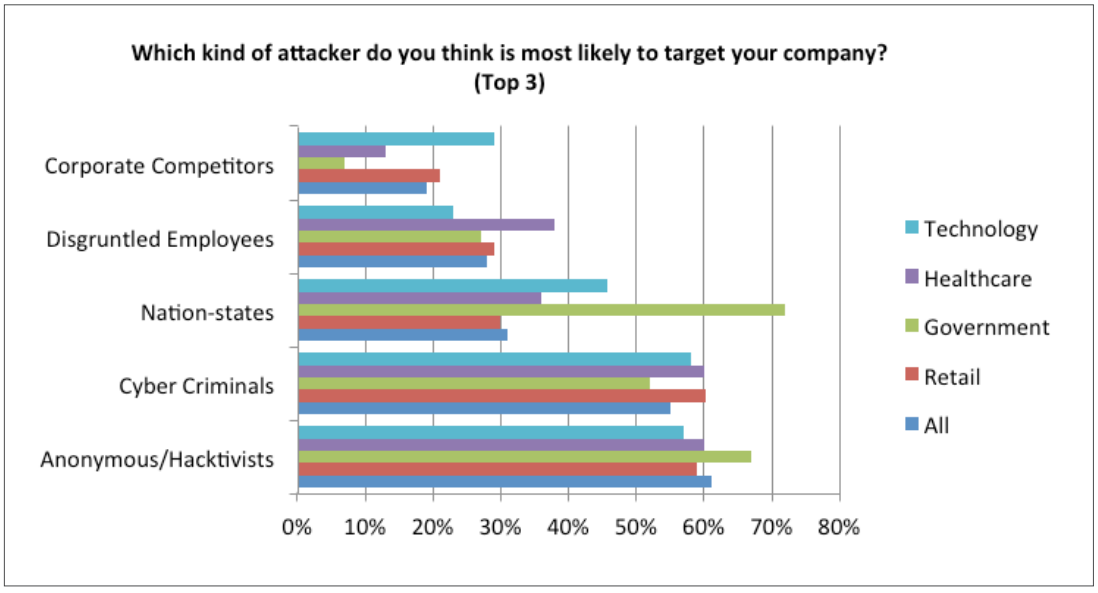


61% of respondents feel that they are most likely to be attacked by Anonymous and/or other hacktivists, for example, those behind such public attacks as those on HBGary Federal, Sony and the Stratfor security consultancy. These attacks can do tremendous damage to the companies' brand and bottom line. Overall, respondents feel that threats from organized crime, including nation states and cybercriminals, are a greater threat than disgruntled employees and corporate competitors.

There was not a wide variation in the perceived sources of threats across market segments, though government security professionals display much more concern about nation state sponsored attacks.

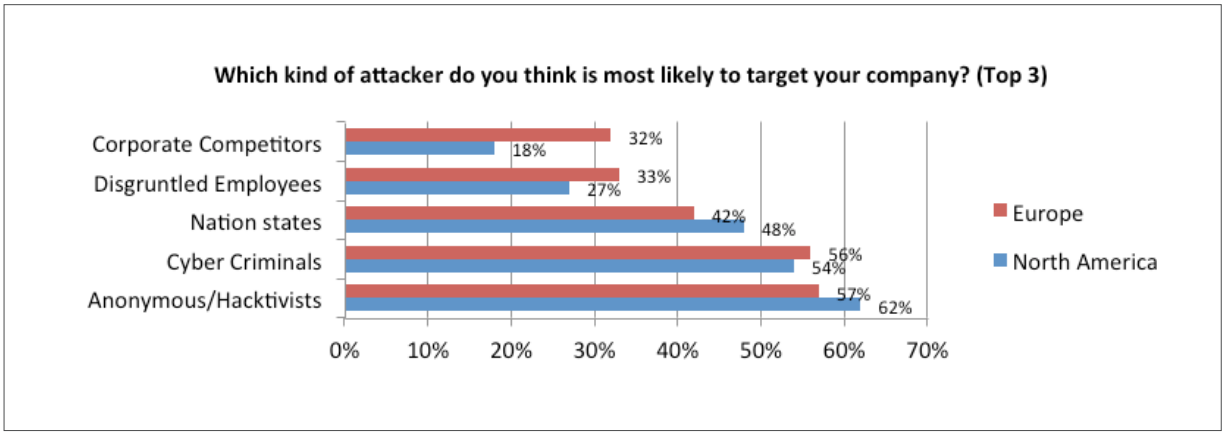
Security professionals from Europe are far more concerned (32%) about attacks from corporate competitors than respondents from North America. In addition, European respondents list intellectual property (IP) as one of the top three most important assets; 60% versus 39% in North America.

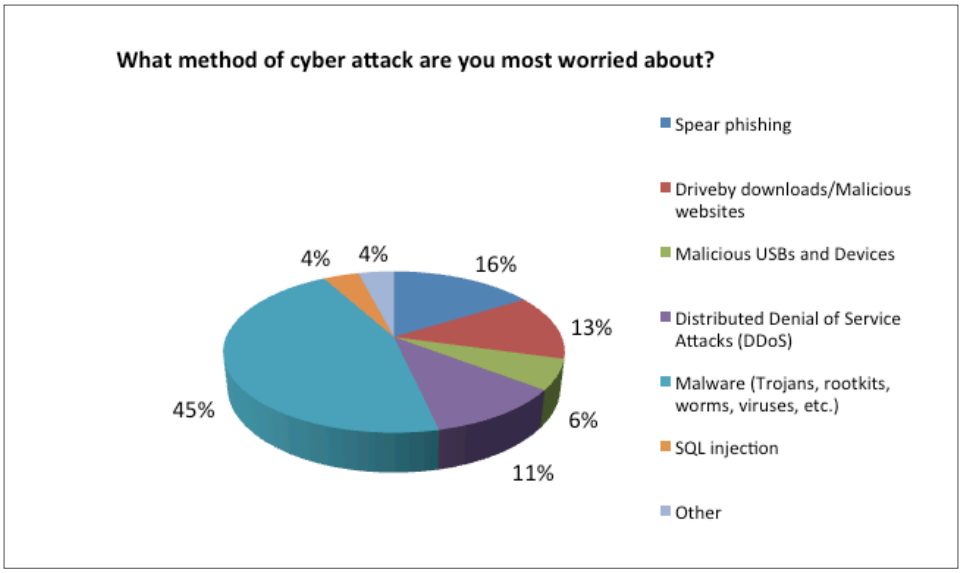




Almost half the respondents, 45%, feel that malware such as Trojans, rootkits, worms, and viruses would be the likely method of cyber attack. The next most cited attack was spear phishing at 16%. Both of these methods are common components of advanced attacks. It was a spear phishing attack that targeted an executive at RSA, a division of EMC, in the recent SecurID token hack. Zero-day malware then leveraged a flaw in a desktop application to install a backdoor.

What the survey makes very clear is that IT and security professionals take seriously their responsibility for reporting security breaches. Almost all (95%) agree that cyber security breaches should be disclosed to customers and the public. Furthermore a significant majority (77%) feel that additional information should be provided, such as what was compromised, and even how the breach occurred (29%). Only 6% of respondents feel that nothing should be disclosed. These results are consistent across market segments and geographies.

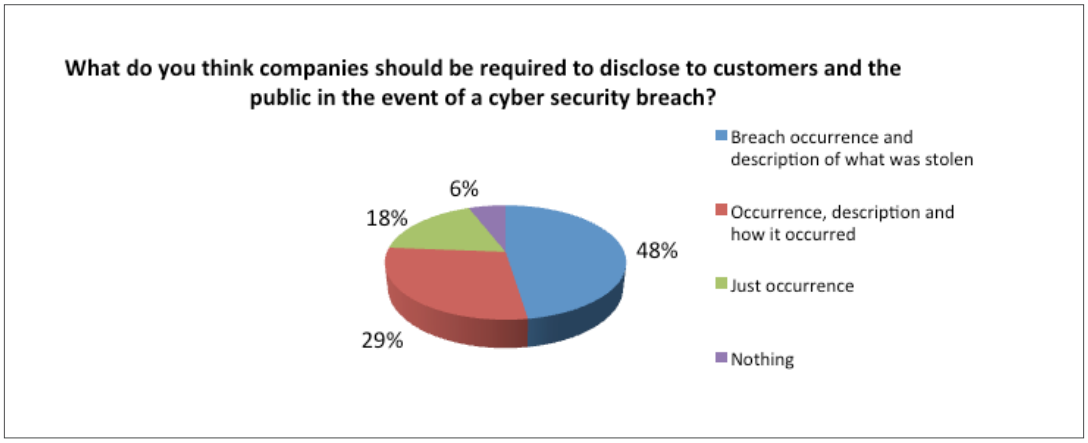


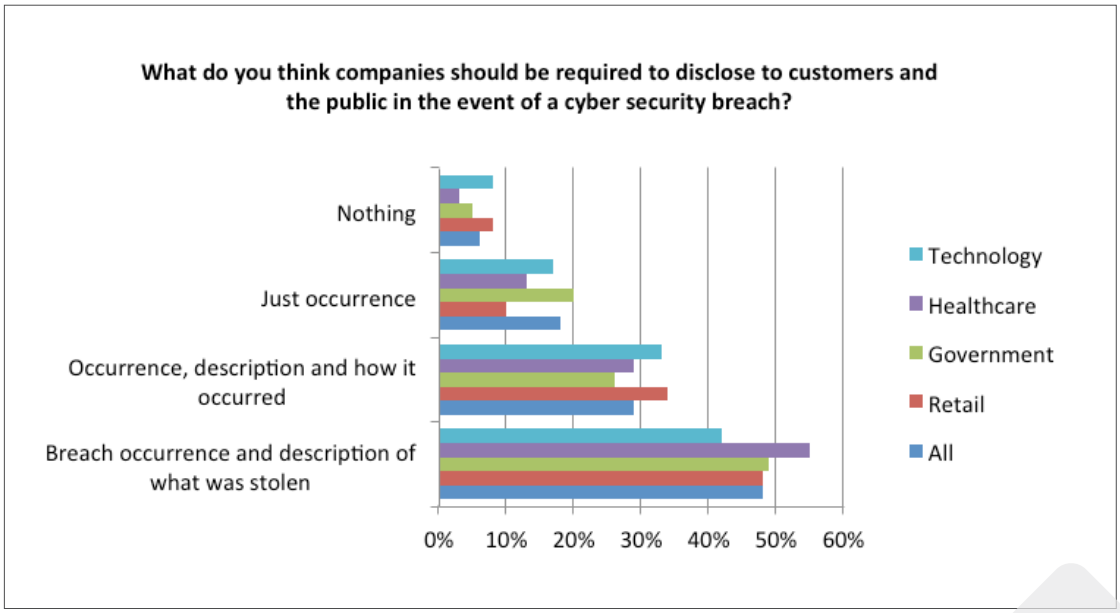


Key Finding #2. IT and security professionals are not confident that their current cyber security is highly effective at protecting their most important and most vulnerable machines.

Infrastructure servers (e.g., domain controllers, DNS servers, credential servers) were identified as the most important—and most vulnerable—machines in the environment by over half of the survey respondents.

Following infrastructure servers, respondents rank file/database, web, and email servers and end-points very similarly in terms of importance. These results are remarkably consistent across market segments. In Europe, respondents list file servers and databases as slightly less important, 33%, than the overall average of 48%.



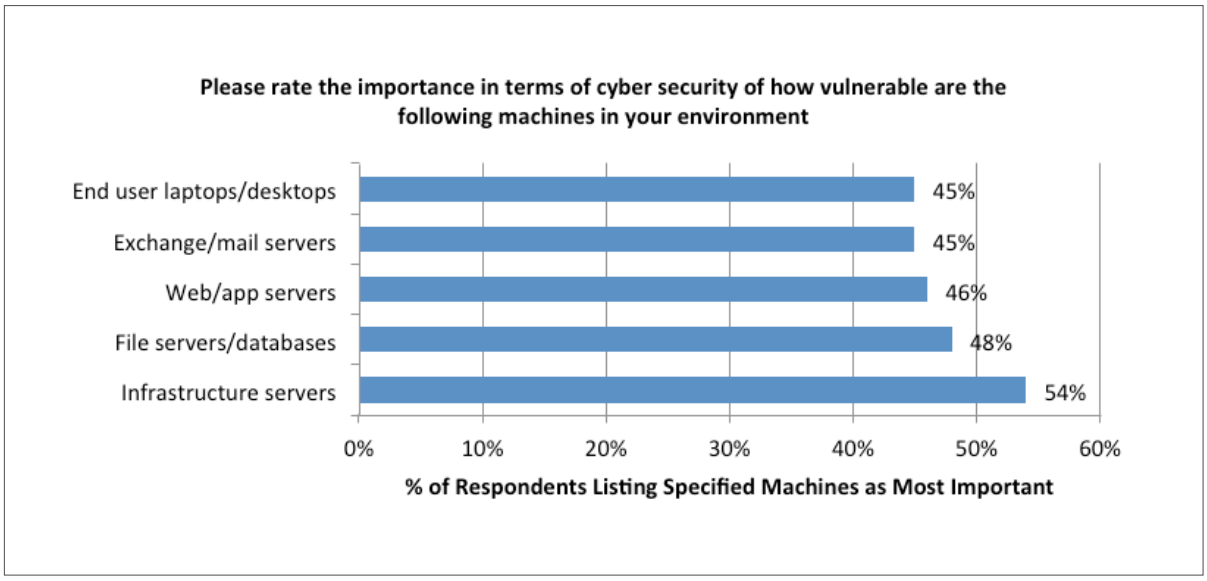


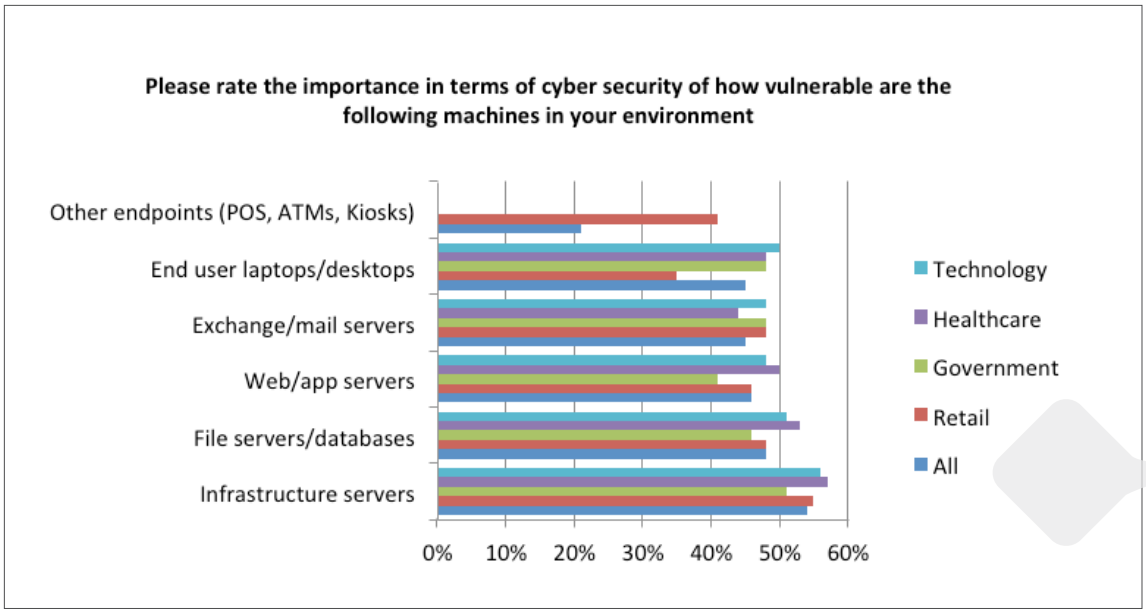
Understandably respondents from retail, hospitality and restaurant organizations are more concerned about the vulnerability of other endpoints such as Point of Sale devices; retail organizations are more concerned about endpoints other than end user laptops (41% vs. 21%).

In contrast, respondents' confidence in their current cyber security posture for protecting these very machines is not high: only 26% of respondents feel that their current cyber security was highly effective in protecting endpoints.

Europeans feel even less confident about their current state of end user cyber security, with only 16% rating their security status as highly effective highly effective, versus 26% in North American.

Even for the self-identified most important and vulnerable infrastructure servers, only 40% of IT and security professionals rate cyber security as highly effective. For the remaining important infrastructure machines, only about a third of respondents feel that their cyber security was highly effective.



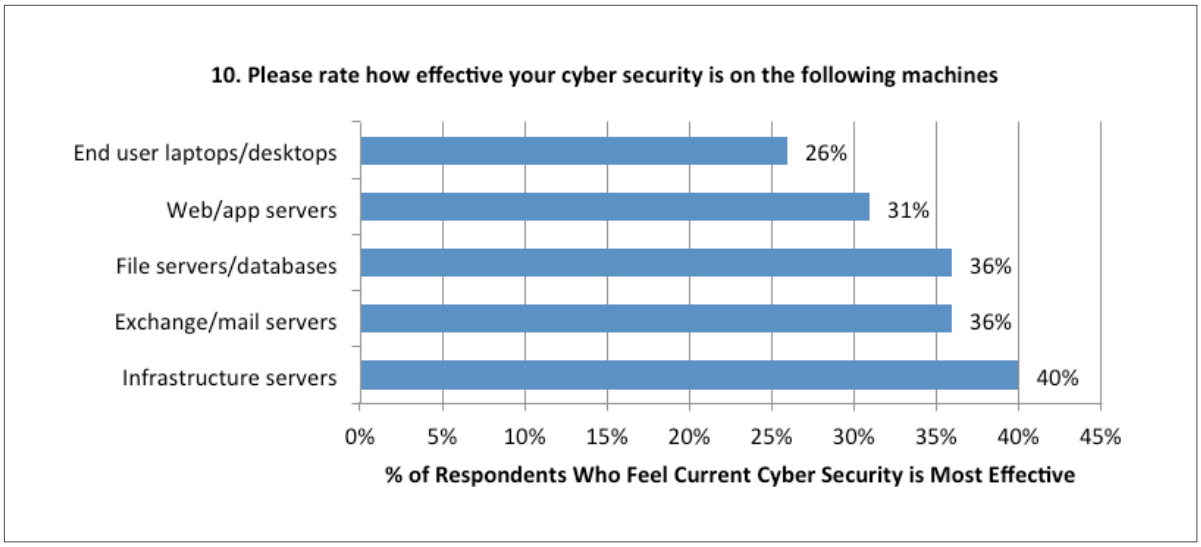


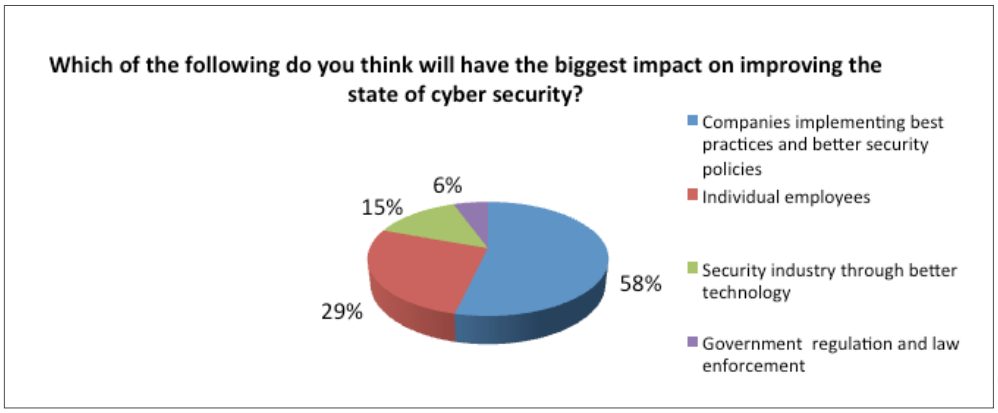
One factor in these relatively low confidence levels is the greater awareness and understanding of advanced threats. Cyber attacks launched by Anonymous/hacktivists, cyber criminals and nation states are posing new challenges to traditional security solutions, such as antivirus software and 'in-flight' Network/Host-based Intrusion Detection systems (NIPS/HIPS). These perpetrators utilize the full spectrum of computer intrusion technologies and techniques and, as mentioned previously, carefully plan and target their attacks. For example, advanced attacks can gain a foothold using zero-day malware which will not be detected by anti-virus software. In advanced persistent threats, the attack is orchestrated over long periods of time, months even years, in order to achieve the defined objectives.

Key Finding #3. IT and security professionals surveyed feel that the implementation of best practices and better security policies have the biggest impact on improving cyber security.

Most respondents feel that implementing best practices and better security policies have the biggest impact on improving the state of cyber security; respondents feel that government regulation will have the least impact.

"Better technology" by itself was identified as having the biggest impact on improving cyber security by only 15% of respondents.





Conclusion

Only 40%

of those surveyed feel that the assets they rate as most important and most vulnerable (the infrastructure servers at the heart of their business) are protected in a highly effectively manner by their current cyber security posture;

Most IT and security professionals believe that their organizations will be the target of an advanced attack within the next six months. These attacks will most likely be perpetrated by Anonymous/hacktivists, cyber criminals and nation states with the requisite skill, organization and funding to utilize the full spectrum of computer intrusion technologies in carefully planned and remotely manipulated attacks.

Only 40% of those surveyed feel that the assets they rate as most important and most vulnerable (the infrastructure servers at the heart of their business) are protected in a highly effectively manner by their current cyber security posture; even fewer (26%) feel confident about the protection afforded end user laptops and desktops. The most anticipated method of cyber attack, by almost half the respondents, is malware.

Use of best practices and better security policies are considered by IT and security professionals to have the biggest impact on improving cyber security against advanced threats—much greater than regulatory solutions; only 6% cited governmental legislation as having any impact on improving security.

This last finding has significant implications for executives responsible for enterprise cyber security: To be most effective, security solutions must follow best practices specific to combating the unique characteristics of advanced threats as well as reflect the security policies of each individual enterprise.

1. Source: Symantec Corporation.

Appendix

2012 Bit9 APT SURVEY
Respondents: 1,861 Countries surveyed: Worldwide
Survey conducted online from March 28, 2012 - April 4, 2012.

1. How many employees does your organization have?

100	329	18%
101-500	308	17%
501-1,000	197	11%
1,001-5,000	357	19%
5,001-10,000	179	10%
10,001+	491	26%
Total	**1861**	**100%**

2. What industry are you in? *(Pick one)*

Education	148	8%
Entertainment/Media	39	2%
Finance/Insurance	247	13%
Government	285	15%
Healthcare	107	6%
Hospitality/Restaurant	40	2%
Manufacturing	125	7%
Pharmaceuticals	19	1%
Retail	83	4%
Technology	436	23%
Utilities/Energy/Telco	112	6%
Other, please specify	220	12%
Total	**1861**	**100%**

3. Where is your company's headquarters? *(Pick one)*

United States	1533	82%
Canada	111	6%
Central America	4	0%
South America	8	0%
UK	39	2%
Germany	16	1%
France	15	1%
Spain	5	0%
Benelux	3	0%
Italy	3	0%
Asia & Australasia	44	2%
Middle East	14	1%
Africa	7	0%
Other	59	3%
Total	**1861**	**100%**

ABOUT Bit9

Bit9, the global leader in Advanced Threat Protection, protects the world's intellectual property (IP) by providing innovative, trust-based security solutions to detect and prevent sophisticated cyber threats. The world's leading brands rely on Bit9's award-winning Advanced Threat Protection Platform for endpoint protection and server security.

Bit9 stops advanced persistent threats by combining real-time sensors, cloud-based software reputation services, continuous monitoring and trust-based application control and whitelisting—eliminating the risk caused by malicious, illegal and unauthorized software.

The company's global customers come from a wide variety of industries, including e-commerce, financial services, government, healthcare, retail, technology and utilities. Bit9 was founded on a prestigious United States federal research grant from the National Institute of Standards and Technology – Advanced Technology Program (NIST ATP) to conduct the research that is now at the core of the company's solutions.

Bit9 is privately held and based in Waltham, Mass. For more information, visit http://www.bit9.com, follow us on Twitter @Bit9, Facebook and Google+, or call +1 617-393-7400.

4. Do you think your company will be targeted by a cyber attack in the next 6 months. *(Pick one)*

Yes	1183	64%
No	678	36%
Total	**1861**	**100%**

5. Which kind of attacker do you think is most likely to target your company in the next 6 months? *(Pick up to 3 responses)*

Anonymous/hactivists	1140	61%
Disgruntled employees	522	28%
Corporate competitors	363	20%
Cyber criminals	1023	55%
Nation state – China	571	31%
Nation state – Russia	235	13%
Nation state – Other fill in	76	4%

6. Please rate each of the following assets in terms of their value to your company. *(Pick your top 3)*

Personal customer information	1120	60%
Customer financial information	944	51%
Company confidential contract/ negotiation information	1028	55%
Intellectual Property -- research/ patents/designs	757	41%
Brand equity/consumer confidence	521	28%
Proprietary data (source code, plans, etc.)	699	38%

7. What should companies be required to disclose to customers/ public in the event of a cyber security breach? *(Pick one)*

That a cyber security breach occurred	330	18%
The cyber security breach occurrence & description of what was stolen	886	48%
The cyber security breach occurrence, description of what was stolen, & information on how the attack occurred	542	29%
Nothing	103	6%
Total	**1861**	**100%**

8. Which of the following do you think will have the biggest impact on improving the state of cyber security? *(Pick one)*

Companies implementing best practices and better security policies	1077	58%
Security industry through better technology	282	15%
Government regulation and law enforcement	139	7%
The individual employees within an organization.	363	20%
Total	**1861**	**100%**

ABOUT BIT9 PARITY

Bit9 Parity is designed to help companies implement best practices and improved security policies for protection against advanced threats—without putting undue burden on IT and security professionals.

- Deployment of application control and whitelisting protection strategies for both applications and devices through a rules engine that allows for flexible configuration of policies and roles-based access control;
- A security policy based on actual, relative risk metrics allows for more informed, targeted policy creation and enforcement; policy simulation to assess the impact of default-deny policies before they are implemented without impeding legitimate enterprise activity;
- Automatic and intelligent correlation of endpoint data through building a library of event correlation experiential knowledge that helps companies better adapt to evolving threats and prevent future attacks.

9. On a scale of 1 to 5, where 1 is the least important and 5 is the most important, please rate the importance in terms of cyber security of how vulnerable the following machines are in your environment: *Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option.*

	Least Important *(1)*	Label *(2)*	Label *(3)*	Label *(4)*	Most Important *(5)*	N/A *(6)*
End user machines (laptops, desktops)	36 *(2%)*	117 *(6%)*	268 *(14%)*	565 *(30%)*	843 *(45%)*	32 *(2%)*
Other endpoints (point of sale, ATMs, kiosks, etc.)	187 *(10%)*	161*(9%)*	283 *(15%)*	349 *(19%)*	382 *(21%)*	499 *(27%)*
Mobile devices	53 *(3%)*	146 *(8%)*	349 *(19%)*	567 *(30%)*	666 *(36%)*	80*(4%)*
Infrastructure servers (e.g. domain controllers, DNS servers, credential servers)	38 *(2%)*	90 *(5%)*	225 *(12%)*	417 *(22%)*	999 *(54%)*	92*(5%)*
Exchange and mail servers	34 *(2%)*	98 *(5%)*	241 *(13%)*	545 *(29%)*	844 *(45%)*	99*(5%)*
Web and business application servers	32 *(2%)*	100 *(5%)*	255 *(14%)*	507 *(27%)*	854 *(46%)*	113 *(6%)*
File servers/databases	40 *(2%)*	99 *(5%)*	260 *(14%)*	466 *(25%)*	888 *(48%)*	108 *(6%)*
Cloud servers (SAAS, IAAS, PAAS)	102 *(5%)*	118 *(6%)*	238 *(13%)*	355 *(19%)*	597 *(32%)*	451 *(24%)*

10. On a scale of 1 to 5, where 1 is the least effective and 5 is the most effective, please rate how effective your current cyber security is on the following machines: *Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option.*

	Least Important *(1)*	Label *(2)*	Label *(3)*	Label *(4)*	Most Important *(5)*	N/A *(6)*
End user machines (laptops, desktops)	58 *(3%)*	134 *(7%)*	420 *(23%)*	731 *(39%)*	481 *(26%)*	37 *(2%)*
Other endpoints (point of sale, ATMs, kiosks, etc.)	82 *(4%)*	101 *(5%)*	314 *(17%)*	421 *(23%)*	319 *(17%)*	624 *(34%)*
Mobile devices	186 *(10%)*	311 *(17%)*	516 *(28%)*	468 *(25%)*	272 *(15%)*	108 *(6%)*
Infrastructure servers (e.g. domain controllers, DNS servers, credential servers)	12 *(1%)*	50 *(3%)*	301 *(16%)*	660 *(35%)*	750 *(40%)*	88 *(5%)*
Exchange and mail servers	20 *(1%)*	42 *(2%)*	323 *(17%)*	695 *(37%)*	679 *(36%)*	102 *(5%)*
Web and business application servers	21 *(1%)*	70 *(4%)*	388 *(21%)*	687 *(37%)*	586 *(31%)*	109 *(6%)*
File servers/databases	18 *(1%)*	65 *(3%)*	334 *(18%)*	694 *(37%)*	675 *(36%)*	75 *(4%)*
Cloud servers (SAAS, IAAS, PAAS)	85 *(5%)*	106 *(6%)*	322 *(17%)*	421 *(23%)*	340 *(18%)*	587 *(32%)*

11. What do you think is the main reason for the increased number of cyber attacks over the past year? *(Pick one)*

Defenses aren't strong enough	332	18%
There are more hackers/ organized criminal groups/ nation state attacks out there than in the past	1225	66%
The number hasn't risen; it's just that there is more media hype surrounding them	304	16%
Total	**1861**	**100%**

12. What method of cyber attack are you most worried about? *(Pick one)*

Spear phishing	307	16%
Driveby downloads/ Malicious websites	243	13%
Malicious USBs and Devices	117	6%
Distributed Denial of Service Attacks (DDoS)	212	11%
Malware (Trojans, rootkits, worms, viruses, etc.)	831	45%
SQL injection	82	4%
Other (fill in)	69	4%

266 Second Avenue Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com

About Bit9, Inc.

Bit9 is the leader in Advanced Threat Protection. The company's award-winning Application Control solutions provide total visibility and control over all software on endpoints, eliminating the risk caused by malicious, illegal, and unauthorized software. Bit9 specializes in protecting organizations against the Advanced Persistent Threat.

Copyright © 2012 Bit9, Inc. All Rights Reserved. Bit9, Inc. and Parity are trademarks or registered trademarks of Bit9, Inc. All other names and trademarks are the property of their respective owners. Bit9 reserves the right to change product specifications or other product information without notice.