StaySafeOnline.org
National Cyber Security Alliance

Symantec™

2011 NATIONAL SMALL BUSINESS STUDY

The National Cyber Security Alliance has conducted a new study with Symantec to analyze cyber security practices, behaviors and perceptions of small businesses throughout the United States. The study was conducted by Zogby International, which polled 1,045 U.S. small business owners from September 19-21, 2011. The survey had a margin of +/- 3.1 percentage points. Key findings of this study are listed below:

Small businesses are increasingly dependent on the Internet:

- Two thirds (66%) say that their business is dependent on the Internet for its day-to-day operations, two fifths of which (38%) characterize it as very dependent with two-thirds (67%) say they have become more dependent on the Internet in the last 12 months.

- Sensitive information businesses report handling includes customer data (69%), half deal in financial records and reports (49%), one quarter (23%) have their own intellectual property and one fifth (18%) handle intellectual property belonging to others outside of the company.

- A majority of small business owners (57%) say that the loss of Internet access for 48 straight hours during a regular business week would be disruptive to their business, two fifths (38%) say it would be extremely disruptive.

Small businesses experience a lack of cyber security authority in practice:

- 77% do not have a formal written Internet security policy for employees and of those who don't most do not have an informal policy either (49%), a majority (56%) do not have Internet usage polices that clarify what websites and web services employees can use, and 63% do not have policies regarding how their employees use social media.

- 60% say they have a privacy policy in place that their employees must comply with when they handle customer information and half (52%) have a plan or strategic approach in place for keeping their business cyber secure.

- More small business owners say they do not (45%) provide Internet safety training to their employees than do (37%).

- Two thirds (67%) allow the use of USB devices in the workplace.

- Six in ten (59%) say they do not require any multifactor authentication for access to any of their networks, and only half (50%) say that all of their machines are completely wiped of data before disposal.

Cyber security is increasingly important to the value of a business:

- Seven in ten (69%) say that Internet security is critical to their business's success.

- A majority (57%) thinks having a strong cyber security and online safety posture is good for their company's brand.

A disconnect exists among U.S. small businesses between perceptions of cyber security preparedness and reality:

- Two fifths (40%) say that if their business suffered a data breach or loss such as loss of customer or employee information, credit or debit card information or loss of intellectual property, their business does not have a contingency plan outlining procedures for responding and reporting it, but a third do (34%).

- Small business owners are most concerned about their employees picking up a computer virus while on the Internet (32%), followed by spyware/malware (17%), loss of data (10%), ID theft (8%), loss of customer information (8%), loss of intellectual property (4%), and seeing objectionable content and loss of employee data (1%). However, a very large majority (85%) say that given the measures they have taken, their company is safe from hackers, viruses, malware, and cyber-security breaches.

- Three quarters (72%) say they would know if their computer network was compromised, but nine in ten (91%) say their company has never suffered a security breach in which important information was stolen from a computer or their network. Of those who did suffer one, the majority says they told their customers about it (57%).

Small businesses are increasingly utilizing mobile devices:

- However, majorities do not let employees access company files/data remotely from mobile devices (72%), work from home computers/access company information from personal mobile devices (59%), or have an employee policy/guidelines in place for remote use on mobile devices (63%).

2011 NCSA / Symantec Small Business Study

National Cyber Security Alliance

Symantec

Zogby International

October 2011

Overview: The National Cyber Security Alliance and Symantec have released their annual Small Business Internet Security Survey, which analyzes cybersecurity behaviors and perceptions of small business owners throughout the nation. The study was conducted by Zogby International, which polled over 1,000 Americans with a margin of +/- 3.1 percentage points.

1. About what percentage of your employees use the Internet every day?

1%-25%	9%
26%-50%	3
51%-75%	5
76%-100%	76
None	6
Not sure	1

2. What do your employees use the Internet for? (Choose all that apply)

Communications with customers	82%
Research	79
Communications with vendors/business partners	70
Procurement	48
Marketing	47
Managing financials and accounting	40
Managing a database	34
Social network presence for company	30
Blogging about company, products, related issues	17
Other	19
Not sure	2

3. Do you have policies around how your employees use social media?

Yes	36%
No	63
Not sure	1

4. Do you have a website for your business?

Yes	60%
No	40
Not sure	<1

5. Do you manage your company's website in-house or is it outsourced?

In-house	67%
Outsourced	32
Not sure	1

6. Do you advertise your services elsewhere on the web other than your own website?

Yes	52%
No	47
Not sure	1

7. What can customers/potential customers do on your site? (Choose all that apply)

Find product information	88%
Request customer service	64
Provide feedback on products and services	41
Make a purchase	33
Make an appointment for a service call	31
Get technical support	26
Make a payment for a service	21
Download a product	13
Access an online service	11
Other	11
Not sure	<1

8. Do you think any customers may have not followed through or abandon a purchase from your website because of a security or safety concern?

Yes	8%
No	74
Not sure	18

9. How dependent on the Internet is your business for its day-to-day operations?

Very dependent	38%	**Dependent**	**66%**
Somewhat dependent	28		
Not very dependent	20	**Not dependent**	**34**
Not at all dependent	14		
Not sure	<1		

10. Has your company become more or less dependent on the Internet in the last 12 months?

Much more dependent	16%	**More dependent**	**67%**
Somewhat more dependent	51		
Somewhat less dependent	10	**Less dependent**	**14**
Much less dependent	5		
Not sure	19		

11. On a scale of 1 to 5, with 1 being not disruptive at all and 5 being extremely disruptive, indicate how disruptive it would be to your business if you lost Internet access for 48 hours in a row during the course of your regular business week?

Not at all disruptive	13%	**Not Disruptive**	**28%**
2	14		
3	15		
4	19	**Disruptive**	**57**
Extremely disruptive	38		
Not sure	<1		

12. Do you have an internal IT manager whose job is solely focused on IT? (i.e. backing up information, managing email accounts and website, updating their software, troubleshooting technology-related issues, etc.)

Yes	15%
No	85
Not sure	<1

13. Who is responsible for IT at your businesses then?

Myself	59%
Outside IT consultant	16
IT-savvy employee	14
No one	6
Outsource to service provider	5
Technology reseller or IT resale partner	<1
Not sure	<1

14. Do you use cloud-based SaaS or file-sharing services for your business?

Yes	10%
No	83
Not sure	7

15. Which of the following cloud-based SaaS or file-sharing services are you currently using for your business? (Choose all that apply)

Back-up	64%
Email	62
Document management	62
Calendar	51
Sales and/or relationship management	28
Project management	27
None/Not sure	2

16. Does your company have a formal written Internet security policy for employees?
17. Does your company have an informal Internet security policy?

<u>Employee Internet Security Policies</u>

	Yes	No	N/A	Not sure
Formal written Internet security policy	15	77	7	1
Informal Internet security policy	42	49	9	1

18. How confident are you that your employees are aware of your formal Internet security policy and practices?

Very confident	82%	**Confident**	**98%**
Somewhat confident	16		
Not very confident	2	**Not Confident**	**3**

19. Does your business have a plan or strategic approach in place for keeping your business cyber-secure?
20. Do you have a privacy policy that your employees must comply with when they handle customer information?

<u>Employee Internet Security Policies</u>

	Yes	No	N/A	Not sure
Plan or strategic approach in place for keeping your business cyber-secure	52	39	7	2
Privacy policy that employees must comply with when they handle customer information	60	28	11	1

21. What type of sensitive information does your business typically handle? (Choose all that apply)

Customer data	69%
Financial records and reports	49
Credit card information	34
Employee personal data	32
Privacy information	31
Intellectual property belonging to company	23
Intellectual property belonging to others	18
Other	14
None	11
Not sure	1

22. Do all of your employees have access to the same information on your network?

Yes	38%
No	52
N/A	10
Not sure	<1

23. How critical would you say that Internet security is to your business's success?

Very critical	32%	**Critical**	**69%**
Somewhat critical	37		
Not very critical	19	**Not critical**	**30**
Not at all critical	11		
Not sure	1		

24. Do you think having a strong cyber security and online safety posture is good for your company's brand?

Yes	57%
No	13
N/A	19
Not sure	11

25. How often do you have the person or people responsible for IT check your company's computers to ensure that all computer software critical to your business including security software (antivirus, anti-spyware, firewalls and operating systems) is up-to-date?

Weekly	52%
Monthly	20
Annually	9
Never	9
Not sure	10

26. Do you provide training to your employees on how to keep their computers secure?

Yes	40%
No	42
N/A	17
Not sure	1

27. On average, how many hours of computer security training do you provide per employee annually?

Less than one hour	13%
One to three hours	34
Three to five hours	16
Five to eight hours	12
More than eight hours	18
Not sure	8

28. Is the computer security training mandatory?

Yes	76%
No	22
Not sure	2

29. Do you provide training for your employees on how to safely use the Internet?

Yes	37%
No	45
N/A	17
Not sure	1

30. On average, how many hours of Internet safety training do you provide per employee annually?

Less than one hour	13%
One to three hours	34
Three to five hours	16
Five to eight hours	12
More than eight hours	16
Not sure	8

31. Is the Internet safety training mandatory?

Yes	75%
No	24
Not sure	1

32. Do you have workplace signage that helps keep IT security and Internet safety awareness top of mind for your employees?

Yes	9%
No	70
N/A	21
Not sure	1

33. Do you have Internet network usage policies that include employee responsibilities to protect your company's data, customer data and your personnel data?

Yes	40%
No	39
N/A	19
Not sure	1

34. Do you have Internet usage polices that clarify what websites and web services employees can use?

Yes	25%
No	56
N/A	18
Not sure	1

35. Have you ever had to discipline an employee for misuse of the Internet, a security incident related to the Internet or a privacy violation?

Yes	14%
No	68
N/A	17
Not sure	1

36. Have you ever had to fire or dismiss an employee for misuse of the Internet, a security incident related to the Internet or a privacy violation?

Yes	5%
No	78
N/A	17
Not sure	1

37. Do you allow the use of USB devices (memory, thumb drives, etc) in the workplace?

Yes	67%
No	20
N/A	12
Not sure	1

38. Do you use any means of multifactor (using more than a password and logon) authentication to access any of the company's online service providers?

Yes	30%
No	54
N/A	14
Not sure	3

39. Do you require any multifactor (using more than a password and logon) authentication for access to any of your networks?

Yes	23%
No	59
N/A	16
Not sure	3

40. What applications, services or data requires additional multifactor authentication? (choose all that apply)

Financial	72%
Network configuration	57
Customer records/orders	57
Personnel/HR	47
Shared file systems	44
Contact relationship management systems	30
Process controls	20
Other	12
Not sure	5

41. Which of the following practices are implemented in your workplace or on the network? (choose all that apply)

All machines are completely wiped of data before disposal	50%
All machines are scanned to be sure they have all protections before joining (rejoining) the network	38
All employees forced to change passwords on a regular interval	24
None of these	21
N/A	17
Not Sure	3

42. What are your company's main sources for information regarding online safety and security? (Choose all that apply)

Website of software or hardware vendor	39%
Peer (other business owner or trusted professional)	28
Internal IT professional	27
Other companies that provide services to small business	21
Technology publication website	16
Trade association newsletter	11
Trade association website	8
Website of a nonprofit group	7
Government website	6
Social Media (Small business forums)	6
Local business association	5
Other	13
N/A	14
Not sure	6

43. Which of the following materials or resources would be most helpful in making your business more cyber-secure? (Choose up to three)

A checklist of best practices for small business	36%
A list of the top ten things any business should do to stay more cyber-secure	25
A plan for what to do in the case of a data breach	20
A model acceptable use and Internet security policy	14
A PowerPoint presentation to train employees	13
A brochure to distribute to employees	10
Case studies on the cyber security practices in small business like yours	8
A glossary of security terms	6
Signage for the workplace on security, privacy and protecting customers	4
Other	5
N/A	26
Not sure	14

44. When you think about the kinds of things that can happen while your employees are on the Internet, what are you most concerned about?

Viruses	32%
Spyware/malware	17

Loss of data	10
ID theft	8
Loss of customer information	8
Loss of intellectual property	4
Seeing objectionable content	1
Loss of employee data	1
Other	2
No concerns	6
N/A	12
Not sure	1

45. Given the measures you have taken, how safe do you think your company is from hackers, viruses, malware or a cyber-security breach?

Very safe	23%	**Safe**	**85%**
Somewhat safe	62		
Not very safe	6	**Unsafe**	7
Not at all safe	1		
N/A	5		
Not sure	3		

46. Do you have a wireless router at your office?
47. Can you log onto your wireless network without entering a password?

Wireless Network

	Yes	No	Not sure
Wireless router at office	73	26	1
Log on without password	18	81	1

48. What percentage of your employees take a laptop, smart phone or tablet that has company info home/off site at night or on weekends?

1-25%	16%
26-50%	5
51-75%	4
76%-90%	2
More than 90%	14
None	57
Not sure	2

49. Do you let your employees use their own mobile phones or devices (tablets, laptops) for business?
50. Can employees use personal mobile phones or devices (tablets, laptops) in the workplace?

Use of Mobile Devices

	Yes	No	Not sure
Employees can use personal mobile devices in workplace	72	25	3

Employees can use own mobile devices for business	52	44	3

51. Do your employees access company files or data remotely from mobile devices (laptop, smart phone, tablet)?
52. Can your employees work from their home computers or access company information from their personal mobile devices (access network, applications, email etc.)?
53. Do you have policies or guidelines for how employees use mobile or remote devices?

Use of Mobile Devices

	Yes	No	Not sure
Employees work from home computers/access company information from personal mobile device	39	59	2
Employee policy/guidelines for remote use on mobile devices	34	63	3
Employees access company files/data remotely from mobile devices	26	72	3

54. Which of the following security solutions do you implement for your network and data when accessed remotely?

We use an encryption solution for critical data	31%
We use a security solution such as VPN	28
Other	16
We don't use security solutions on remotely accessed data	17
Not sure	9

55. Would you know if your computer network was compromised (i.e. infected with a virus, private information stolen, etc.)?
56. Has your company ever suffered a security breach in which important information was stolen from a computer or your network?
57. Did you let your customers know about the security breach?

Security Breaches

	Yes	No	Not sure
Would you know if your computer network was compromised?	72	6	22
Has your company ever suffered a security breach in which important information was stolen from a computer on your network?	4	91	4
Did you let your customers know about the security breach?	57	37	7

58. Are you more concerned about an internal threat to your company such as an employee, ex-employee, or contractor/consultant stealing data, or an external threat such as a hacker or cyber-criminal stealing data?

External threat	53%

Internal threat	10
Both	11
Neither	24
Not sure	3

59. How satisfied are you with the amount of security you provide to protect customer or employee data?

Very satisfied	41	**Satisfied**	**87%**
Somewhat satisfied	46		
Somewhat dissatisfied	3	**Dissatisfied**	**4**
Very dissatisfied	1		
N/A	8		
Not sure	1		

60. If your business suffered a data breach or loss such as loss of customer or employee information, credit or debit card information or loss of intellectual property, does your business have a contingency plan outlining procedures for responding and reporting?

Yes	34%
No	40
N/A	21
Not sure	5

61. Do you let your customers and partners/suppliers know what you do to protect their information or data?

Yes	34%
No	43
N/A	19
Not sure	4

62. Which of the following best describes the steps you take to protect customer and employee data?

We have multiple layers of computer security	37%
We have a minimal threshold of security	18
We rely on someone outside the company take care of it for us	12
We don't take any steps to protect customer or employee data	4
Other	8
N/A	17
Not sure	4

63. Do you use encryption for your customer data?

Yes	29%
Considered it, but never implemented	9
No	39

No, but would be interested in it	3
N/A	17
Not sure	4

64. How strongly do you agree or disagree that your customers are concerned about the IT security of your business?

Strongly agree	16%	**Agree**	**44%**
Somewhat agree	28		
Somewhat disagree	19	**Disagree**	**36**
Strongly disagree	17		
N/A	15		
Not sure	6		

65. If you conduct commerce online, have you limited any portion of it because of security issues?

Yes	16%
No	38
Do not conduct commerce online	45
Not sure	2

66. Do you think your company's data is safer or less safe than it was 12 months ago?

Safer	24%
Less safe	11
About the same	57
N/A	6
Not sure	2

67. Do you agree or disagree that your Internet service provider provides you with adequate cyber-security protections?

Strongly agree	12%	**Agree**	**59%**
Somewhat agree	47		
Somewhat disagree	17	**Disagree**	**25**
Strongly disagree	8		
N/A	7		
Not sure	9		

68. Which of the following best describes your thoughts on cyber-security?

Cost of doing business	53%
A nice thing to have	23
Overhead	5
Competitive differentiator	3
None of these	12
Not sure	5

69. Which anti-virus/security software came pre-bundled on your computers? (Choose all that apply)

Norton	36%
McAfee	32
Microsoft	21
Symantec	16
AVG	8
Trend Micro	5
Kapersky	4
Cisco	1
Other	7
N/A	10
Not sure	12

70. Are the computers in your organization connected to a server-based network?

Yes	34%
No	58
N/A	4
Not sure	4

71. If you had extra money to put toward improving your company's software infrastructure, which area would you consider most important?

Back-up	23%
System recovery	18
Information security	11
Data loss prevention	9
Software patching/updating	3
Going green	3
OS migration	2
User assistance, system diagnostics and	2
Asset discovery and tracking	1
Software license audit and compliance	1
Other	4
N/A	12
Not sure	11

72. What is your biggest obstacle to implementing more robust cyber-security solutions for your business?

No additional funds to invest	32%
Lack of clarity about what would be the best protections for my business	12
Don't believe an investment in cyber security will yield any returns	10
Lack of time to devote to the issue	8
Don't have the technical skills or knowledge	4
Finding a trusted third party that really understands cyber security and my needs	3

Don't know how to create a cyber security plan	1
Time to train staff	1
Other	4
N/A	17
Not sure	7

73. What vendor website do you use most frequently to make your cyber-security solutions purchases?

Norton	19%
AVG	11
McAfee	10
Symantec	8
Microsoft	8
Trend Micro	3
Kaspersky	3
Cisco	1
Computer Associates	<1
Other	9
N/A	16
Not sure	11