



# 2012 NCSA / Symantec

# National Small Business Study

**National Cyber Security Alliance**

**Symantec**

**JZ Analytics**

October 2012

## Methodology and Sample Characteristics

JZ Analytics was commissioned by the National Cyber Security Alliance (NCSA) and Symantec to conduct an online safety survey of 1,015 U.S. small and mid-sized businesses (SMBs) nationwide. A sampling of JZ Analytics' online panel, which is an aggregate representation of American SMBs (250 employees or less), was invited to participate from September 27, 2012 to September 29, 2012. The margin of error is +/- 3.1 percentage points and margins of error are higher in sub-groups. The MOE calculation is for sampling error only.

## Narrative Analysis

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

**Table 1. Internet Reliance**

| | Employees |
|---|---|
| 1-25% | 18% |
| 26-50% | 5% |
| 51-75% | 5% |
| 76-100% | 59% |
| None | 10% |
| Not sure | 3% |

**2.** For what types of activities do your employees use the Internet?

**Table 2. Employee Activities**

| | Activities |
|---|---|
| Communications with customers | 68% |
| Research | 68% |
| Communications with vendors/business partners | 50% |
| Procurement | 23% |
| Marketing | 36% |
| Sales and customer relationship management | 33% |
| Managing financials and accounting | 31% |
| Managing a database | 18% |
| Website maintenance | 25% |
| Social network presence for company | 26% |
| Blogging about company, products, related issues | 12% |
| Other | 16% |
| Not sure | 3% |

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

| | |
|---|---|
| Very dependent | 45% |
| Somewhat dependent | 26% |
| Not very dependent | 14% |
| Not at all dependent | 15% |
| Not sure | <1% |

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

| | |
|---|---|
| Much more dependent | 17% |
| Somewhat more dependent | 48% |
| Somewhat less dependent | 9% |
| Much less dependent | 8% |
| Not sure | 17% |

**5.** 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?

| | |
|---|---|
| 1 Not disruptive at all | 18% |
| 2 | 10% |
| 3 | 16% |
| 4 | 17% |
| 5 Extremely disruptive | 38% |
| Not sure | 2% |

**6.** Do you have a website for your business?

| | |
|---|---|
| Yes | 46% |
| No | 54% |

**7.** What can customers/potential customers do on your site?

**Table 3. Customer Activities on Website**

| | Activities |
|---|---|
| Find product/service information | 82% |
| Request customer service | 56% |
| Provide feedback on products and services | 37% |
| Make a purchase | 38% |
| Make an appointment for a service call | 21% |
| Get technical support | 12% |
| Make a payment for a service | 24% |
| Download a product | 9% |
| Access an online service | 12% |
| Other | 13% |

| | |
|---|---|
| Not sure | 3% |

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

| | |
|---|---|
| Website managed in-house | 69% |
| Website management is outsourced | 29% |
| Not sure | 2% |

**9.** How critical would you say that a safe and trusted Internet is to your business's success?

| | |
|---|---|
| Very critical | 46% |
| Somewhat critical | 27% |
| Not critical | 24% |
| Not sure | 3% |

**10.** Do you think having a strong cybersecurity and online safety posture is good for your company's brand?

| | |
|---|---|
| Yes | 77% |
| No | 23% |

**11.** Do you agree or disagree that your customers are concerned about the IT security of your business?

| | |
|---|---|
| Strongly agree | 16% |
| Somewhat agree | 28% |
| Somewhat disagree | 19% |
| Strongly disagree | 22% |
| Not sure | 15% |

**12.** If your business were to suffer a data breach, what kind of impact do you think it would have?

| | |
|---|---|
| Long-term negative impact | 10% |
| Short-term impact | 32% |
| No impact, it would be viewed as an isolated incident | 47% |
| Not sure | 11% |

**13.** Which of the following would have a lasting impact on your business?

| | |
|---|---|
| Data theft | 30% |
| Malware/virus | 45% |
| Corporate website being hacked | 13% |
| Denial of service attack | 20% |
| Using your brand for phishing | 27% |
| None | 25% |
| Not sure | 12% |

**14.** Do you have an internal IT manager whose job is solely focused on technology-related issues?

| | |
|---|---|
| Yes | 10% |
| No | 90% |

**15.** Who is responsible for online and cybersecurity are your business?

| | |
|---|---|
| Myself | 66% |
| Outside IT consultant | 8% |
| IT savvy employee | 9% |
| No one | 11% |
| Outsourced to a service provider | 4% |
| Technology related reseller or IT resale partner | <1% |
| Not sure | 3% |

**16.** Does your company have a formal written Internet security policy for employees?

| | |
|---|---|
| Yes | 10% |
| No | 87% |
| Not sure | 3% |

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

| | |
|---|---|
| Very confident | 62% |
| Somewhat confident | 30% |
| Not at all confident | 3% |
| Not sure | 5% |

**18.** Does your company have an informal Internet security policy?

| | |
|---|---|
| Yes | 28% |
| No | 69% |
| Not sure | 3% |

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

| | |
|---|---|
| Yes | 23% |
| No | 75% |
| Not sure | 2% |

**20.** Does your business have a written plan in place for keeping your business cyber-secure?

| | |
|---|---|
| Yes | 14% |
| No | 83% |
| Not sure | 3% |

**21.** Do you have a privacy policy that your employees must comply with when they handle customer or employee information?

| | |
|---|---|
| Yes | 38% |
| No | 60% |
| Not sure | 2% |

**22.** What type of sensitive information does your business typically handle?

**Table 4. Sensitive Information**

| | Information |
|---|---|
| Customer data | 53% |
| Financial records and reports | 35% |
| Credit card information | 30% |
| Employee personal data | 23% |
| Intellectual property | 24% |
| Intellectual property belonging to others | 14% |
| Other | 10% |
| None | 22% |
| Not sure | 3% |

**23.** Do all of your employees have access to all the information on your network or do you limit access?

| | |
|---|---|
| Yes, employees have access to all of the information on our network | 36% |
| No, employee access is limited on our network | 56% |
| Not sure | 8% |

**24.** How often are your company's computers checked to ensure that all computer software is up-to-date?

| | |
|---|---|
| Weekly | 44% |
| Monthly | 20% |
| Annually | 10% |
| Never | 14% |
| Not sure | 13% |

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

| | |
|---|---|
| Yes | 29% |
| No | 68% |
| Not sure | 4% |

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

| | |
|---|---|
| Yes | 29% |
| No | 68% |
| Not sure | 4% |

**(If Q26 = Yes)**
**27.** Do you provide training internally or externally?

| | |
|---|---|
| Internally | 77% |
| Externally | 5% |
| Both internally & externally | 16% |
| Not sure | 1% |

**28.** On average, how many hours of computer security training do you provide per employees annually?

| | |
|---|---|
| Less than 1 hour | 14% |
| 1-3 hours | 38% |
| 3-5 hours | 16% |
| 5-8 hours | 5% |
| More than 8 hours | 18% |
| Not sure | 9% |

**29.** Is the computer security training mandatory?

| | |
|---|---|
| Yes | 81% |
| No | 19% |
| Not sure | 1% |

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

| | |
|---|---|
| Yes | 28% |
| No | 70% |
| Not sure | 2% |

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

| | |
|---|---|
| Less than 1 hour | 13% |
| 1-3 hours | 39% |
| 3-5 hours | 15% |
| 5-8 hours | 7% |
| More than 8 hours | 20% |
| Not sure | 7% |

**32.** Is Internet safety training mandatory?

| | |
|---|---|
| Yes | 80% |
| No | 19% |
| Not sure | 1% |

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

| | |
|---|---|
| Yes | 11% |
| No | 87% |
| Not sure | 2% |

**34.** Do you have Internet usage policies that specify which websites and Web services employees can use?

| | |
|---|---|
| Yes | 17% |
| No | 81% |
| Not sure | 2% |

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

| | |
|---|---|
| Yes | 9% |
| No | 90% |
| 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 | 94% |
| Not sure | 1% |

**37.** Do you use any cloud (SaaS [i.e. Dropbox]/web-based/hosted) services for your business?

| | |
|---|---|
| Yes | 18% |
| No | 80% |
| Not sure | 3% |

**38.** Which of the following cloud (SaaS/web-based/hosted) services are you currently using for your business?

**Table 5. Cloud Services**

| | |
|---|---|
| Back-up | 54% |
| Email | 43% |
| Document management | 50% |
| Calendar | 31% |
| Security | 15% |
| Sales and/or relationship management | 14% |
| Project management | 17% |
| None | 2% |
| Not sure | 3% |

**39.** Are you considering moving any of your software applications to the cloud to enhance software security?

| | |
|---|---|
| Yes | 10% |
| No | 78% |
| Not sure | 13% |

**40.** Do you use file-sharing services for your business?

| | |
|---|---|
| Yes | 14% |
| No | 82% |
| Not sure | 4% |

**41.** Which of the following file-sharing services are you currently using for your business?

**Table 6. File Sharing Services**

| | |
|---|---|
| Back-up | 49% |
| Email | 56% |
| Document management | 65% |
| Calendar | 34% |
| Security | 24% |
| Sales and/or relationship management | 23% |
| Project management | 20% |
| None | 1% |
| Not sure | 2% |

**42.** Do you use any means of multifactor/strong/two-factor authentication (using more than a password and logon) to access any of the company's online service provider?

| | |
|---|---|
| Yes | 19% |
| No | 75% |
| Not sure | 6% |

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

| | |
|---|---|
| Yes | 14% |
| No | 80% |
| Not sure | 6% |

**44.** What applications services or data require additional multifactor authentication?

**Table 7. Authentication**

| | |
|---|---|
| Financial | 63% |
| Network configuration | 39% |
| Customer records/orders | 52% |
| Personnel/HR | 32% |

| | |
|---|---|
| Shared file systems | 33% |
| Contact relationship management systems | 22% |
| Process controls | 15% |
| Other | 9% |
| Not sure | 10% |

**45.** Do you have an automated system that requires employees to change passwords at a pre-determined interval?

| | |
|---|---|
| Yes | 14% |
| No | 83% |
| Not sure | 3% |

**46.** How likely do you think that any of your customers may not have followed through or abandoned a purchase from your website because of a security or safety concern regarding their personal information?

| | |
|---|---|
| Very likely | 2% |
| Somewhat likely | 7% |
| Somewhat unlikely | 11% |
| Very unlikely | 65% |
| Not sure | 15% |

**47.** Would you know if your computer network was compromised (i.e. infected with a virus, private information stolen, etc.)?

| | |
|---|---|
| Yes | 66% |
| No | 18% |
| Not sure | 16% |

**48.** Has your company ever suffered a security breach in which important information was stolen from a computer or your network?

| | |
|---|---|
| Yes | 3% |
| No | 93% |
| Not sure | 3% |

**49.** Did you let your customers know about the security breach?

| | |
|---|---|
| Yes | 5% |
| No | 15% |
| Not applicable | 78% |
| Not sure | 1% |

**50.** Are you 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?

| | |
|---|---|
| Internal threat | 2% |
| External threat | 16% |
| Both | 10% |

| | |
|---|---|
| Neither | 66% |
| Not sure | 7% |

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

| | |
|---|---|
| Very satisfied | 52% |
| Somewhat satisfied | 34% |
| Somewhat unsatisfied | 3% |
| Very unsatisfied | 3% |
| Not sure | 9% |

**52.** Do you agree or disagree that you are doing enough or making enough investments to protect customer data?

| | |
|---|---|
| Strongly agree | 46% |
| Somewhat agree | 37% |
| Somewhat disagree | 5% |
| Strongly disagree | 2% |
| Not sure | 10% |

**53.** Do you agree or disagree that you are doing enough or making enough investments to protect employee data?

| | |
|---|---|
| Strongly agree | 50% |
| Somewhat agree | 33% |
| Somewhat disagree | 4% |
| Strongly disagree | 2% |
| Not sure | 11% |

**54.** Do you agree or disagree with the following statement: Our company is taking enough measures to adequately protect our customers' data?

| | |
|---|---|
| Strongly agree | 51% |
| Somewhat agree | 33% |
| Somewhat disagree | 5% |
| Strongly disagree | 2% |
| Not sure | 10% |

**55.** Do you agree or disagree with the following statement: Our company is taking enough measures to adequately protect our customers' employee data?

| | |
|---|---|
| Strongly agree | 51% |
| Somewhat agree | 31% |
| Somewhat disagree | 4% |
| Strongly disagree | 2% |
| Not sure | 12% |

**56.** If your business suffered a data breach such as: loss of customer or employee information; loss of credit or debit card information; or loss of intellectual property, is there a contingency plan outlining procedures for responding and reporting?

| | |
|---|---|
| Yes | 31% |

| | |
|---|---|
| No | 59% |
| Not sure | 11% |

**57.** Do you let customers know what you do to protect their information or data?

| | |
|---|---|
| Yes | 33% |
| No | 60% |
| Not sure | 7% |

**58.** Do you let your partners/suppliers know what you do to protect their information or data?

| | |
|---|---|
| Yes | 27% |
| No | 67% |
| Not sure | 7% |

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

**Table 8. Steps to Protect Customer/Employee Data**

| | |
|---|---|
| We have multiple layers of computer security | 28% |
| We have a minimal threshold of security | 22% |
| We rely on someone outside of the company to take care of it | 8% |
| We don't take any steps to protect customer or employee data | 6% |
| Other | 6% |
| Not applicable | 26% |
| Not sure | 5% |

**60.** Do you use encryption for your customer data?

| | |
|---|---|
| Yes | 23% |
| Considered, but never implemented it | 10% |
| No, but would be interested | 7% |
| No | 25% |
| Not applicable | 27% |
| Not sure | 7% |

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

| | |
|---|---|
| Yes | 55% |
| No | 40% |
| Not sure | 4% |

**62.** Before disposing of any computer or IT device, are they completely wiped of data?

| | |
|---|---|
| Yes | 75% |
| No | 17% |
| Not sure | 9% |

**63.** Before any new computer or IT device is connected to your computer network, is a scan conducted to ensure it has all the necessary protections?

| | |
|---|---|
| Yes | 69% |
| No | 24% |
| Not sure | 8% |

**64.** Do you automatically scan machines that come into your network to ensure that the security software is up to date?

| | |
|---|---|
| Yes | 62% |
| No | 28% |
| Not sure | 10% |

**65.** Do you have a wireless network at your office?

| | |
|---|---|
| Yes | 67% |
| No | 31% |
| Not sure | 2% |

**66.** Can someone log onto your wireless network without entering a password?

| | |
|---|---|
| Yes | 6% |
| No | 94% |
| Not sure | <1% |

**67.** What percentage of your employees take a laptop, smartphone or tablet containing company information out of the office at night or on weekends?

**Table 9. Employees & Company Information**

| | |
|---|---|
| 1-25% | 25% |
| 26-50% | 4% |
| 51-75% | 4% |
| 76-90% | 2% |
| More than 90% | 11% |
| Not sure | 3% |
| Employees ma not take a device out of the office that has company data | 47% |
| Not sure | 8% |

**68.** Do you let your employees use their personal smartphones or Internet enabled devices (tablets, laptops) for business?

| | |
|---|---|
| Yes | 36% |
| No | 62% |
| Not sure | 3% |

**69.** Can employees use personal smartphones or other Internet enabled devices (tablets, laptops) for nonbusiness usage in the workplace?

| | |
|---|---|
| Yes | 46% |
| No | 51% |
| Not sure | 3% |

**70.** Do your employees access company files or data remotely from Internet enabled devices (laptops, smartphone, tablet) through a cloud (SaaS/web-based/hosted) service like Dropbox?

| | |
|---|---|
| Yes | 14% |
| No | 82% |
| Not sure | 4% |

**71.** Have any of your company laptops been lost or stolen in the last 12 months?

| | |
|---|---|
| Yes | 1% |
| No | 97% |
| Not sure | 1% |

**72.** Can your employees work from their home network connected PC or laptop to access company information (access network applications, email, etc.)?

| | |
|---|---|
| Yes | 30% |
| No | 68% |
| Not sure | 2% |

**73.** Do you have policies or guidelines for how employees use mobile or remote devices?

| | |
|---|---|
| Yes | 25% |
| No | 72% |
| Not sure | 4% |

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

**Table 10. Security Solutions**

| | |
|---|---|
| We use an encryption solution for critical data | 14% |
| We use a security solution such as a VPN | 9% |
| We use a Web based solution such as Log Me In | 9% |

| | |
|---|---|
| We don't use security solutions on remotely accessed data | 33% |
| Other | 16% |
| Not sure | 18% |

**75.** What safety concerns are you most concerned about for your business?

**Table 11. Concerns**

| | |
|---|---|
| Viruses | 24% |
| Spyware or malware | 14% |
| Loss of data | 10% |
| ID theft | 6% |
| Loss of customer information | 5% |
| Loss of intellectual property | 2% |
| Seeing objectionable content | 1% |
| Loss of employee data | <1% |
| Hacking | 5% |
| Cyber attacks | 3% |
| Other | <1% |
| No concerns | 10% |
| Not applicable | 14% |
| Not sure | 6% |

**76.** 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 | 31% |
| Somewhat safe | 45% |
| Not very safe | 3% |
| Not at all safe | 1% |
| Not applicable | 13% |
| Not sure | 7% |

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

| | |
|---|---|
| Safer than it was 12 months ago | 48% |
| Less safe than it was 12 months ago | 8% |
| Not applicable | 27% |
| Not sure | 17% |

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

| | |
|---|---|
| Cost of doing business | 42% |
| A nice thing to have | 21% |
| Overhead | 6% |
| Competitive differentiator | 1% |
| None of these | 18% |
| Not sure | 11% |

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

**Table 12. Software Infrastructure**

| | Employees |
|---|---|
| Back-up | 24% |
| System recovery | 11% |
| Information security | 10% |
| Data loss prevention | 8% |
| Software patching/updating | 2% |
| Going green | 4% |
| OS migration | <1% |
| User assistance and system diagnostics | <1% |
| Asset discovery and tracking | <1% |
| Software license audit and compliance | <1% |
| Other | 3% |
| Not applicable | 21% |
| Not sure | 16% |

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

**Table 13. Cyber-security Solutions**

| | |
|---|---|
| No additional funds to invest | 29% |
| Lack of clarity about what would be the best protection | 10% |
| Don't believe cyber security investment will yield any return | 6% |
| Lack of time to devote to the issue | 5% |
| Don't have the technical skills or knowledge | 4% |

| | |
|---|---|
| Finding a trusted 3rd party that understands cybersecurity & my needs | 2% |
| Don't know how to create a cybersecurity plan | 1% |
| Time to train staff | <1% |
| Other | 3% |
| Not applicable | 29% |
| Not sure | 10% |

**81.** Do you have policies and permissions in place to manage access to company information and/or services (i.e. network services, client lists, intellectual property) when an employee is terminated?

| | |
|---|---|
| Yes | 32% |
| No | 63% |
| Not sure | 6% |

**82.** Do you have policies and permissions in place to manage access to company information and/or services (i.e. network services, client lists, intellectual property) when an employee is changing positions?

| | |
|---|---|
| Yes | 25% |
| No | 69% |
| Not sure | 6% |

**(If Q80 = Yes)**
**83.** If someone were to leave your organization would you do any of the following?

**Table 14. Departed Employee**

| | |
|---|---|
| Eliminate their account | 41% |
| Automatically change their password | 34% |
| Forward their email to another employee | 18% |
| Delete their user information | 35% |
| Other | 7% |
| None of these | 28% |
| Not sure | 9% |

**84.** Do you allow employees to create news accounts for online services without your permission?

| | |
|---|---|
| Yes | 6% |
| No | 90% |
| Not sure | 4% |

**85.** Do you allow employees to download any apps they want to on company smartphones?

| | |
|---|---|
| Yes | 10% |
| No | 84% |
| Not sure | 6% |

**86.** If a trusted third party such as your Internet service provider, your financial institution, a favorite e-commerce site or online service provider knew that a computer on your company's network was infected with a virus or malware do you agree or disagree that you would want them to notify you?

| | |
|---|---|
| Strongly agree | 63% |
| Somewhat agree | 18% |
| Somewhat disagree | 3% |
| Strongly disagree | 2% |
| Not sure | 14% |