

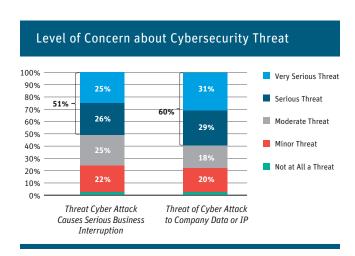
EVIDENCE OF CYBERSECURITY BREACHES ABOUND IN OUR DAILY LIVES – BOTH AT WORK AND AT HOME.

Alarming stories in the press and comprehensive reports, such as Verizon's 2013 Data Breach Investigations Report, serve as daily reminders that we need controls in place and constant vigilance to prevent considerable losses in data, funds and intellectual property.

Due to widespread concern about the issue, Silicon Valley Bank decided to poll our clients about how they're addressing this clear and present risk – with revealing results from the unique perspective of technology companies themselves.

Cybersecurity Risk is Real - and Growing

Most survey respondents believe cybersecurity is a serious threat to both their data and business continuity, with a full 51% rating the threat to business interruption as very serious or serious. The threat to data or intellectual property (IP) was viewed as more significant with 60% saying it was a very serious or serious threat. Software companies are more likely than those in healthcare and cleantech/hardware to consider a cyber attack a serious threat in terms of business interruption (58% versus 47% and 41%, respectively).



"If our security fails, it has the strong potential to destroy the company. We take that risk very seriously."

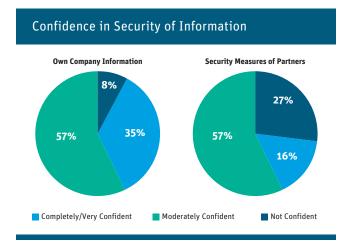
CEO, Cloud Infrastructure Company



MOST TECH AND HEALTHCARE **EXECUTIVES VIEW CYBER** ATTACKS AS A SERIOUS THREAT, NOT JUST HYPE.

Only 35% are Completely or Very Confident About Their Own Security, and Even Less Confident About **Business Partners**

Overall, companies express confidence in the security of their information, but only 35% are completely/very confident, while 57% are moderately confident. Survey respondents were far less confident about the security measures taken by their critical business partners, including vendors, distributors and customers, with only 16% completely/ very confident.

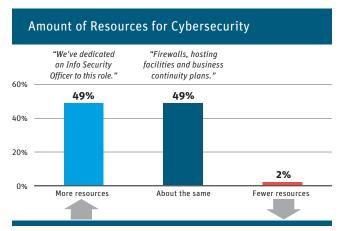


"I believe it will be an ever-increasing concern and challenge. We are particularly concerned about foreign states who attempt to hack into our businesses."

CEO, Consumer Electronics Company

98% of Companies Are Maintaining or Increasing **Security Resources**

Of those 98%, half say they've increased resources (time or money) devoted to the problem this year.

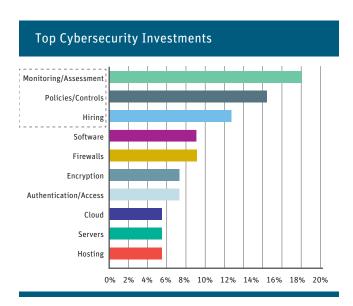


"Way too much resource must be spent managing and defending, which prevents time better spent on innovation and growth. Very sad state for the technology community."

CEO, Big Data Company

Resources Focus on When, Not if, Attack Occurs

Notably, companies are currently investing more in measures to respond to inevitable attacks — monitoring, preventive policies, training and staffing - than in preventative infrastructure. This is consistent with executives describing an increase in the magnitude of cyber attacks, not only in frequency but also in the severity of highly organized attacks from rogue nations.



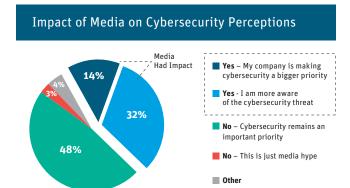
"It's a constant battle that won't go away and we are now spending more to protect ourselves from when we are hacked than to try and keep from being hacked."

CEO, Financial Technology Company



Media Coverage Makes an Impact

For nearly half of executives surveyed, increased media attention to cyber attacks has changed the tide of opinions on cybersecurity and has helped heighten its priority in companies across the board. In addition to risks to their intellectual property and business interruption, they may be keenly aware of the mounting customer concern that comes from rising media exposure - which in turn creates even more incentive to beef up cybersecurity resources.

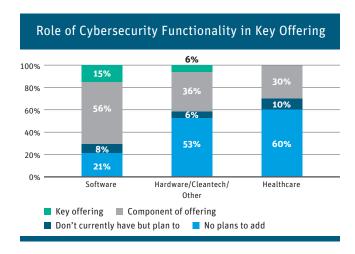


"Although there is a lot of useless media hype, cybersecurity is important and should never be ignored. For the foreseeable future, cyber attacks will be a daily constant for any company with an Internet presence."

CEO, Hardware/Cleantech Startup

Most Companies Have Security Aspect to Product

Attention to cybersecurity now cuts to the core of what companies do. Over half of respondents say cybersecurity is at least one component of their product offering. Not surprisingly, software companies are most likely to offer a cybersecurity component to their product.

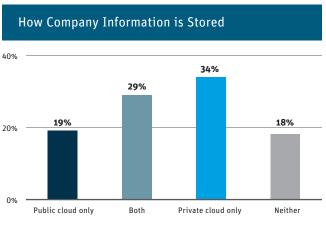


"Cybersecurity is an important issue, and needs to be integrated into every aspect of the running of the company."

CEO, Enterprise Applications Startup

Not Everyone is Embracing the Cloud's "Public" Nature

Most respondents say they still store company information either privately or only partially on the cloud, showing a lower appetite for using the public cloud – even with security measures in place - to cost-effectively store important company information. While 52% are storing information privately, nearly half are using the public cloud for at least some of their data. Software companies are the most aggressive users, with 59% using the public cloud for at least some of their data-likely one reason why they are the sector most concerned about IP and business risk, and most influenced by media coverage. Early-stage companies are also more likely to embrace the cloud, presumably to lower their costs and achieve efficiencies even at a small scale.



"Data security is and always will be an important part of technology infrastructure. The cloud is not a silver bullet."

CEO, IT Services Startup

Study Methodology

Results for Silicon Valley Bank's cybersecurity study were collected through an online survey conducted from July 16-29, 2013. The survey was completed by 216 C-level tech and healthcare clients, 65% of whom are President/CEO. Industry distribution of respondents is 43% software, 20% healthcare, 14% consumer Internet and digital media, 8% hardware and 7% clean technology. Seventy-five percent of respondent companies are startups and 20% in growth stage. Over 60% are based on the west coast. All figures in this report are based on the unweighted responses to closed-ended questions, except the statistics in the Top Security Investments graph, which are based on the classification of free-form open-ended comments typed by survey participants.

About Silicon Valley Bank

Silicon Valley Bank is the premier bank for technology, life science, cleantech, venture capital, private equity and premium wine businesses. SVB provides industry knowledge and connections, financing, treasury management, corporate investment and international banking services to its clients worldwide through 28 U.S. offices and six international operations. (Nasdaq: SIVB) www.svb.com.



Silicon Valley Bank 3003 Tasman Drive Santa Clara, CA 95054 T 408 654 7400 svb.com