As technology evolves, new risks drive innovation in cybersecurity
As the digital industry scrambles to keep up with the pace of innovation, we’re seeing dramatic new opportunities in the cybersecurity space. Spending, venture capital investment, and mergers and acquisitions are on the rise, and we expect this trend to continue.
High-profile cyberattacks dominated the headlines in 2014, with the Sony Pictures hack putting an exclamation point on a breach-heavy year. The sobering reality: Many CEOs believe the worst is yet to come.

That’s because the very technologies that are making our lives easier and more productive are also introducing new and unique security threats — emphasizing the need for security providers to unleash their own wave of innovation. In conversations with clients in the innovation and security space, SVB Analytics is seeing a dramatic evolution in this important tech sector, with both startups and established security providers playing critical roles.
Cyberattacks are on the rise as the value of online data increases.

The amount of data we generate as a society is staggering. And it’s accelerating fast, as new mobile and online technologies change the way people live, work and play. But it comes with a cost. As we grow more comfortable storing our financial, health and other confidential data online, the value of that information — and the incentives to steal it — increases. This is exposing companies throughout the digital economy to increasingly sophisticated, and costly, cyberattacks.

As data use continues to skyrocket, security breaches are growing at a similar pace.

32% Anticipated growth in cloud data center traffic per year through 2018

60,000+ Cyber incidents reported by federal agencies in 2013 — up from 10,000 in 2006

$3.5 million Average cost of a data breach in 2014, up 15% from 2013

Breaches are common in all major data-driven industries, with threats coming from multiple sources.

Highly vulnerable industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>57%</td>
</tr>
<tr>
<td>Technology</td>
<td>13%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>13%</td>
</tr>
<tr>
<td>Financial services</td>
<td>52%</td>
</tr>
</tbody>
</table>

Of existing data requiring protection:

52% is vulnerable

This includes:
- Corporate financial data
- Personally identifiable information (PII)
- Medical records
- User account information

Data breaches since 2013

- 13% caused by malicious insiders
- 25% caused by accidental loss
- 57% caused by malicious outsiders
The popularity of smartphones, tablets and other non-PC devices continues to grow unabated.

**23%**
Anticipated annual growth in Internet traffic through 2018, with majority coming from non-PC devices¹

**1 billion+**
Employee-owned smartphones and tablets in the workplace by 2018⁶

Machine-to-machine traffic (M2M) is expected to increase rapidly as the Internet of Things (IoT) continues to evolve, with connected devices becoming more common for both consumers and businesses.

**84%**
Anticipated annual increase in M2M traffic¹
The enterprise IT landscape continues to evolve, presenting new security challenges.

With each new innovation comes new security vulnerabilities. Smartphones and tablets, cloud computing and connected devices make us more productive and efficient, but sit outside the protection of a corporate firewall. Protecting these data escape points, or endpoints, requires nimble security solutions that most legacy approaches can’t handle.

Before
Priority: Secure enterprise network behind firewall

Cloud computing is moving companies’ mission-critical information onto shared data servers, making security a mutual responsibility between organizations and cloud providers.
Agile startups are leading the charge against emerging security threats, but they aren’t going it alone.

Fast-adapting startups may be the answer. Startups are agile enough to quickly focus research and development (R&D) on specific problems within the broader security landscape. Incumbent security providers aren’t as flexible, but typically have the distribution muscle to get products to market fast. This is creating a new dynamic in the security space, one in which startups develop new security technologies, which are then acquired by incumbents looking to strengthen their existing product suites.

A new security dynamic is emerging
Case study: BYOD/Mobile device management

Startups
Develop targeted solutions for security problems

Incumbents
Incumbents acquire startups and incorporate products

Enterprise customers
Latest security makes it to enterprises faster

Startups that develop an effective security solution still have to successfully market and distribute the product to end users. Incumbents offer a convenient alternative, acquiring many of these startups and merging the solutions into their existing sales channels. This dynamic can be seen in the mobile device management space.

Overall investments are up in the cybersecurity space.

$2 billion
Annual deal volume in 2014 — a 300% increase since 2009

Incumbents are increasingly leaving R&D to startups.

At early stages, startups focus spending on R&D, but as revenue ramps, spending shifts dramatically toward sales and marketing.

2.4 to 1
Median ratio of sales and marketing to R&D investments at public security companies with less than $1 billion in annual revenue

Cybersecurity report | SVB Analytics
The evolution of technology is spurring a “super cycle” of investment in the security space.

The pace of innovation is accelerating, and every advance in technology comes with new and unique security challenges. More and more, businesses are being forced to confront the fact that legacy security infrastructure is not sufficient to meet today’s needs. These realities are driving demand for the next generation of security solutions designed to protect the digital foundation upon which our interconnected society is built.

Consumers and businesses are producing and storing a staggering amount of increasingly valuable data every day. This, coupled with the rapid rise and dynamic nature of new technology, fuel an ecosystem that will continue to drive increased spending, venture capital investment, and merger and acquisition activity for the foreseeable future.
About SVB Analytics

For more than 30 years, Silicon Valley Bank (SVB) has helped innovative companies and their investors move bold ideas forward, fast. SVB provides targeted financial services and expertise through its offices in innovation centers around the world. With commercial, international and private banking services, SVB helps address the unique needs of innovators. Forbes named SVB one of America’s best banks (2015) and one of America’s best-managed companies (2014).

Learn how SVB Analytics provides strategic advisory, research and valuation services for investors and companies in the global innovation economy.

Contact our team of industry experts today.

800.760.9644
svba@svb.com

1 Cisco Global Cloud Index, 2014.
4 Breach Level Index.
7 CB Insights.
8 Silicon Valley Bank internal research.

SVB Analytics is a member of SVB Financial Group and a non-bank affiliate of Silicon Valley Bank. Products and services offered by SVB Analytics are not FDIC insured and are not deposits or other obligations of Silicon Valley Bank. SVB Analytics does not provide tax or legal advice. Please consult your tax or legal advisors for such guidance.

©2015 SVB Financial Group. All rights reserved. Silicon Valley Bank is a Member of FDIC and Federal Reserve System. SVB®, SVB>Find a way, SVB Financial Group, and Silicon Valley Bank are registered trademarks.