RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ECO-W03

Cyber Security for Start-ups: An Affordable 10-Step Plan

David Cowan

Partner
Bessemer Venture Partners
@davidcowan

Acknowledgements


What, Me Worry?

“Startups don't like friction to get their job done. Security feels like friction.”

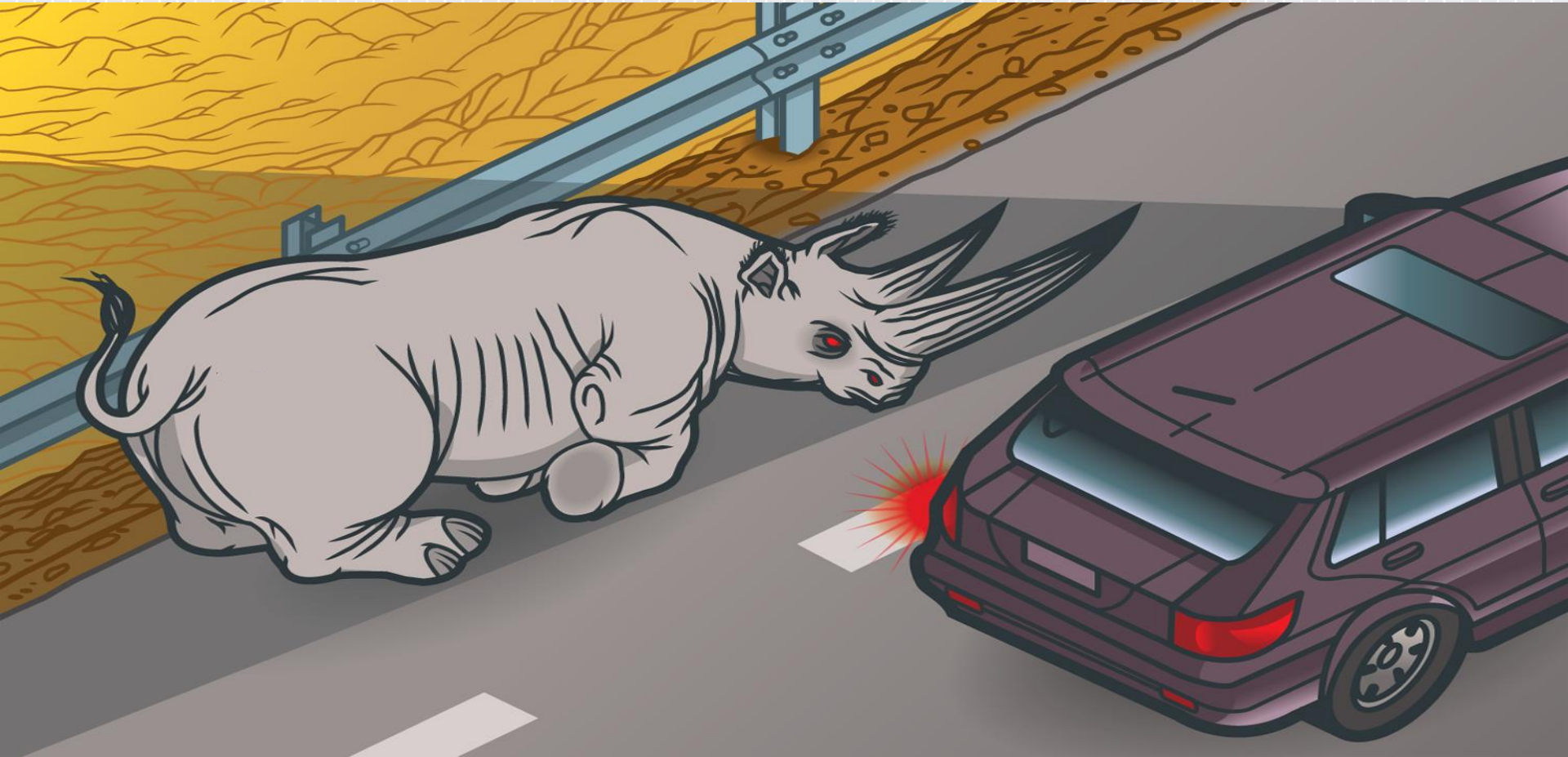
- Ajay Varia, VP Eng, Piazza

Brian Birch, Symantec

"Startups are incredibly vulnerable to cyber attacks in their first 18 months. If a business thinks that it's too small to matter to cybercriminals, then it's fooling itself with a false sense of security."

*20% of small businesses in Canada **reported** falling victim to cyber crimes in the prior 12 months.*

Stolen IP



Defaced

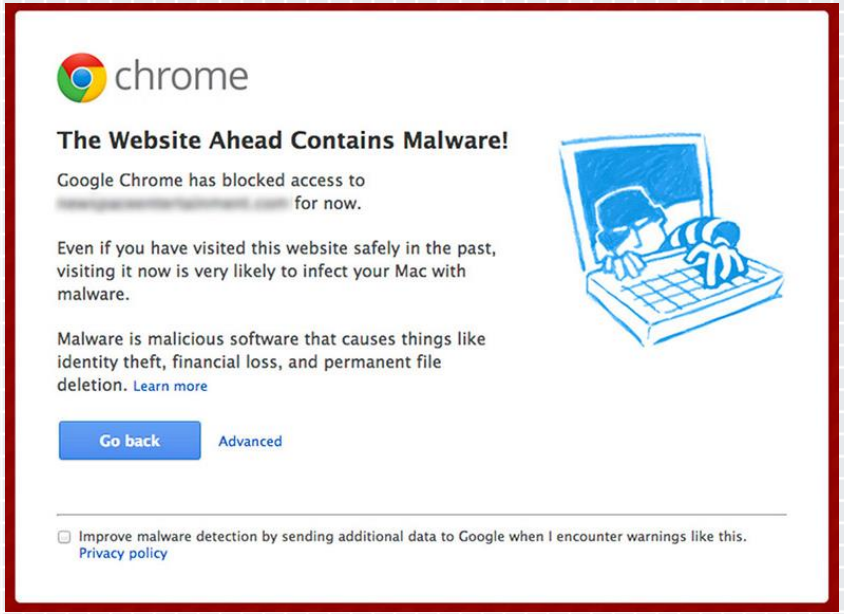
Blacklisted

CREDITNERDS.COM

WordPress

DreamHost

THE WORKFORCE CONSULTANTS



Marketplace Fraud

DOXed

DDoS Outages

"When our API collapsed under a DDoS attack, we experienced more customer churn in that one day than we had in the entire two years since our launch."

Lost Passwords and Payment Data

Compromised Partners

Security Companies Owned!

HBGary

MT.GOX

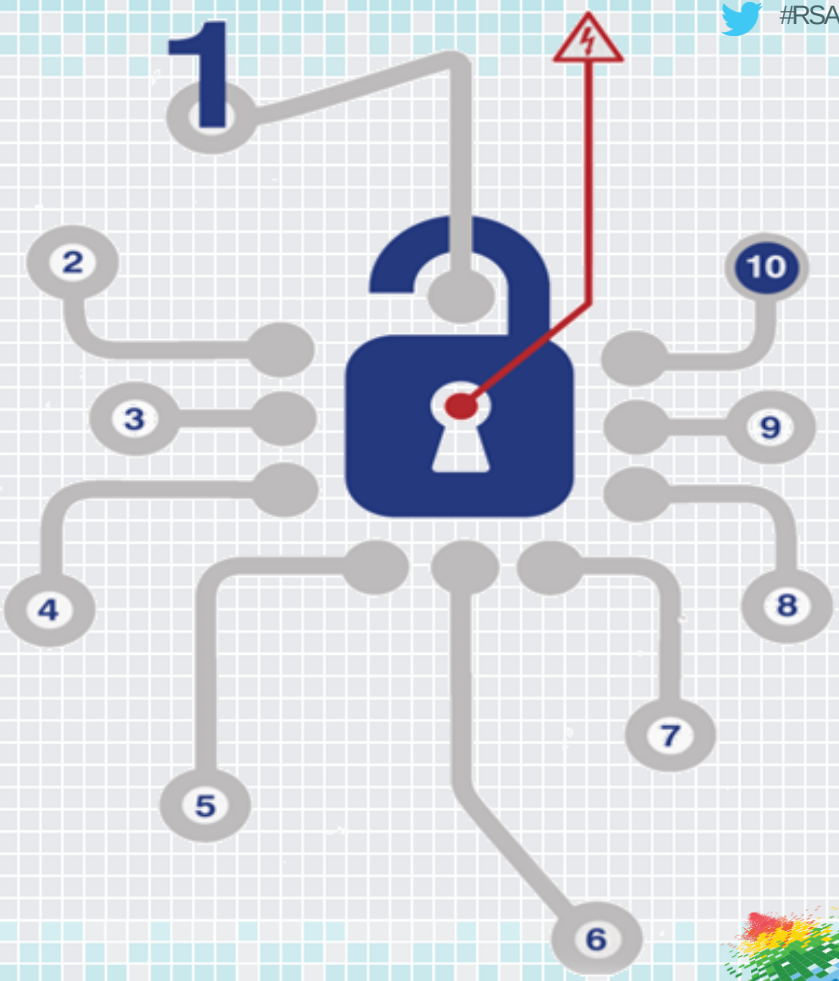
LastPass

Yik Yak

flexcoin

The Ten Steps

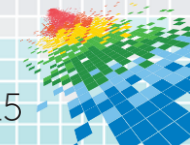
1. Business Cyber Risk Analysis
2. Embrace Security in Your Culture
3. Select the Right Platforms
4. Email is the Master Key
5. Your Web Site is the Front Door
6. Secure Coding
7. Control the Internal Network
8. Physical Security
9. Plan for Failure
10. Be Open with the Public



1. Business Cyber Risk Analysis

With so many ways to hack our systems, why do we even bother?

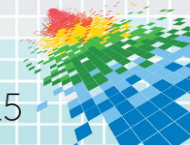
- A. Just do the “standard stuff”
- B. It’s silly to go halfway – close every vulnerability.
- C. Resistance is futile – don’t bother.
- D. Choose the battles based on risk and cost.



Some Common Threats

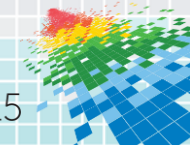
Stolen or leaked IP
Stolen funds
Stolen computer resources
Stolen business information
Account data breach
Employee information
Email dump

DDoS attack
Cyber bombs, back doors
Marketplace fraud
Physical theft / sabotage
Audio surveillance
Brand phishing



Threatscape

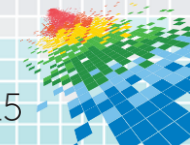
THREAT	LIKELIHOOD	LOSS / INCIDENT	EXPECTED LOSS
Large DDoS Attack **(50+ Gbps for 2+ hours)**	1.2 incidents / year (based on industry averages)	Lost gross margin $2k Remediation $100k 10% churn $2,000k (based on 10% drop in market value)	$2.522M / year



Defense Plan

1. Large DDoS Attack

Detection:	Configure load balancer alerts, server load alerts, and auto-search Twitter for keywords “outage” “crashed” and “site down”, $120/year
Prevention:	DDoS protection service, $60k/year
Remediation:	
Pre-breach	Prepare outage page and key customer contact list.
Post-breach	Cutover to protection service Redirect to temporary outage screen Blog post, and reach out directly to major customers
New Likelihood:	1.2 / year
New Loss / Incident:	$500 lost gross margin, no churn
Net Expected Loss:	$61k / year (97% mitigation)



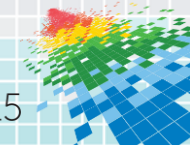
2. Embrace Security in Your Culture

Thousands of decisions are made every day. Culture is how you, as say a leader of the company, are confident that every one of those decisions is the right one.

– Jeff Lawson, Founder of Twilio

2. Embrace Security in Your Culture

- ✓ Share the BCRA with all employees.
- ✓ Schedule periodic training sessions.
- ✓ Create an easy reporting mechanism (e.g. security@yourstartup.com) for any employee to report suspicious activities.
- ✓ Adopt single-sign-on and password management tools
- ✓ Schedule penetration testing on a regular basis – ideally once a quarter (about a $20k expense) – and each “pen test” should simulate targeted phishing attacks on your employees. (K2)



3. Select the Right Platforms

4. Your Email is the Master Key

Forgot Your Password?

Enter Your Email Address

jane.doe@jedix.com

Continue ▸

4. Your Email is the Master Key

5. Your Web Site is the Front Door

Web site

Mobile App

Shoppers, prospective employees, journalists, reviewers, partners, bloggers, investors

Raiding the Cash Register

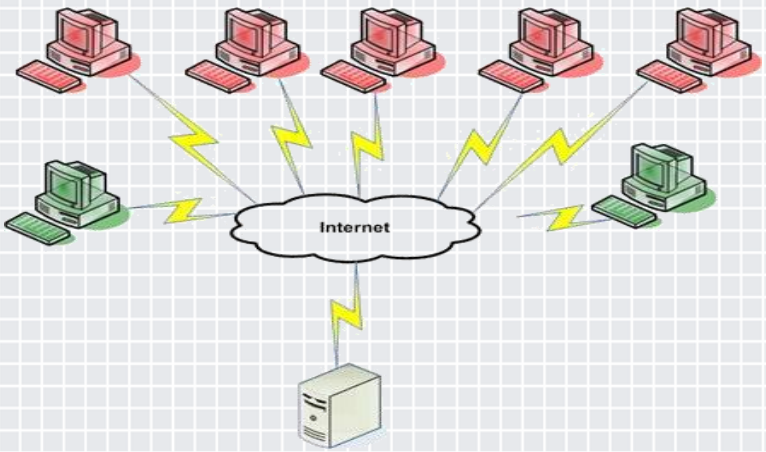
Robbing Your Customers

Deploy a web application firewall. Secure your API with expiring tokens, critical checks in C++ and validated app store receipts.

Defrauding Your Customers

Seek out scams and use device ID to keep the fraudsters out.

Burning Down the Store



Mitigate malware attacks with secure coding practices.

Mitigate DDoS attacks with cloud-based services.

Peter Offringa
Zoosk

"I wish we had put in better DDoS prevention. The size of site that's a target is getting smaller and smaller. Addressing an attack is not something you want to do on the fly."

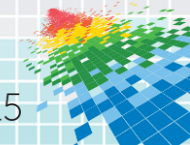
6. Secure Coding

It's less effective and more costly to retrofit security.

Training

- ✓ check the size of user inputs
- ✓ perform and document explicit error checking on all input
- ✓ filter input streams for malicious characters or sequences
- ✓ manage memory
- ✓ sanitize output
- ✓ initialize and clear variables
- ✓ for SQL use stored procedures or pre-compiled PREPAREDSTATEMENTs

Trainers: senior devs, outside experts, or online videos.

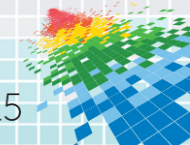


- ✓ Static Code Analysis
- ✓ Dynamic Code Analysis
- ✓ Third Party Libraries, SDKs, APIs

7. Secure the Internal Network

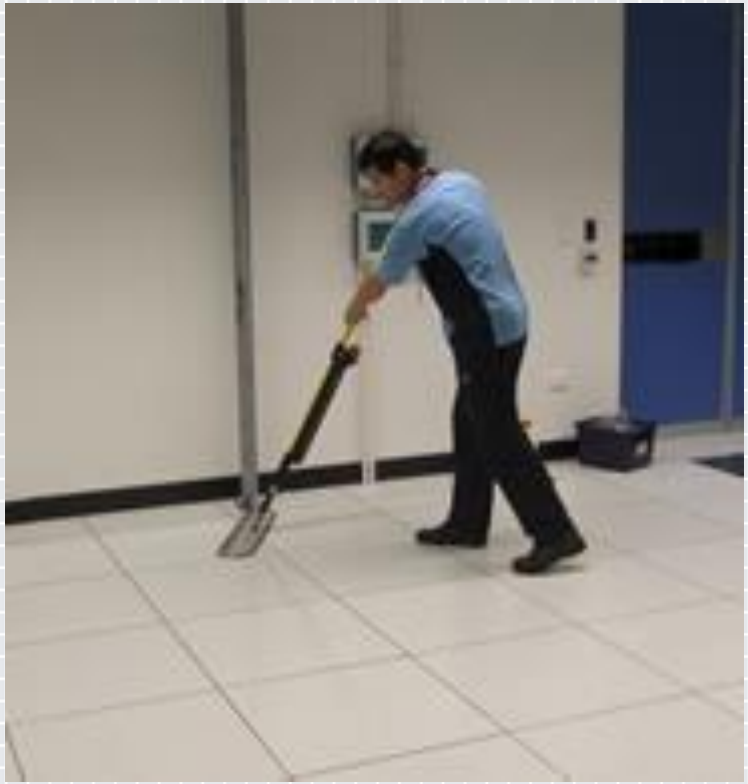
- ✓ Control and Visibility
- ✓ Encrypted, Verified, Archived Backups
- ✓ Collect and Read Logs for Devices, DNS, DHCP
- ✓ Weekly Vulnerability and Port Scans
- ✓ Automated and Manual Patching
- ✓ Restrict and Monitor Admin Accounts
- ✓ Funnel all Outgoing Data Through a Proxy
- ✓ Penetration Testing

Much more: http://www.sans.org/critical-security-controls/controls



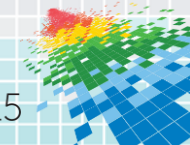
8. Physical Security

- ✓ Make people buzz in.
- ✓ Sign in guests, issue them badges.
- ✓ Put video surveillance in common areas.
- ✓ Clean your own server closet.



9. Plan for Failure

47 states have data breach notification laws, but most SMBs do not have a data breach plan.



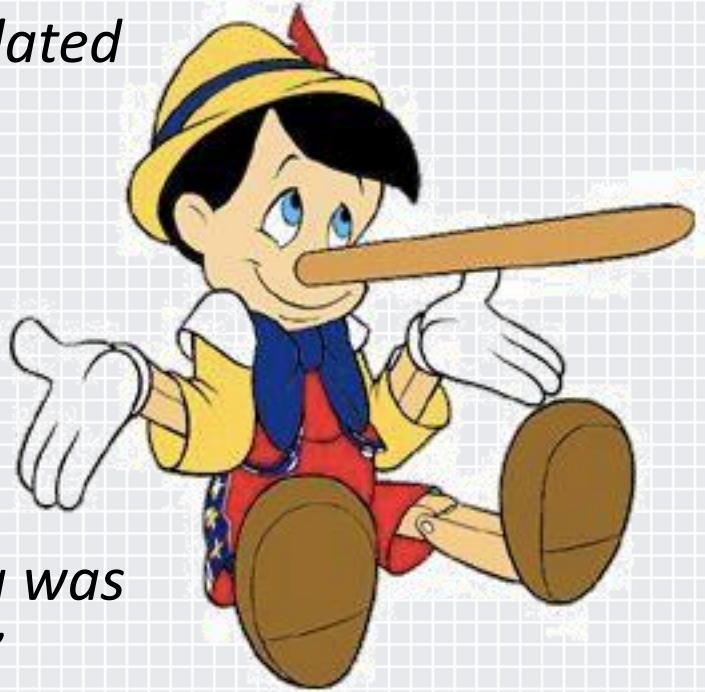
10. Be Open With the Public

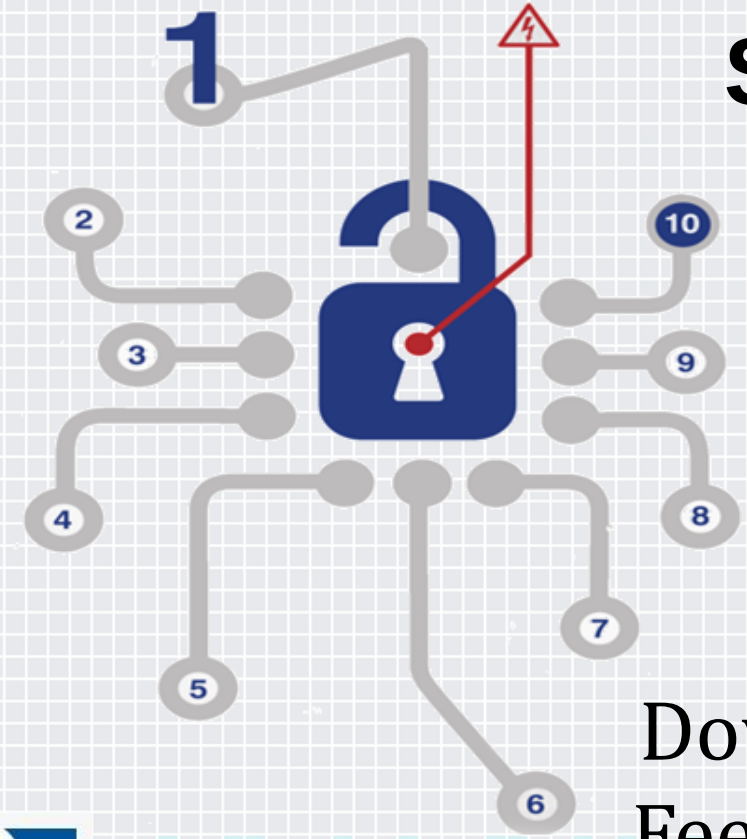
"…some users may have experienced isolated incidents of slow web page rendering."

"It was user error."

"It was our vendor's fault."

"We have no evidence that exposed data was used to harm our customers in any way."





Security for Startups

The *Affordable*
Ten-Step Plan
To Survival
in Cyberspace

Download at bvp.com/cyber
Feedback to cyber@bvp.com