

*You're only as secure as
your weakest supplier*

John Redeyoff

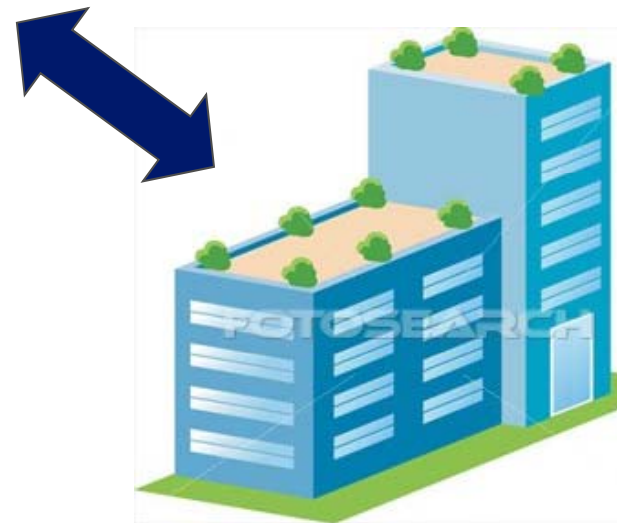
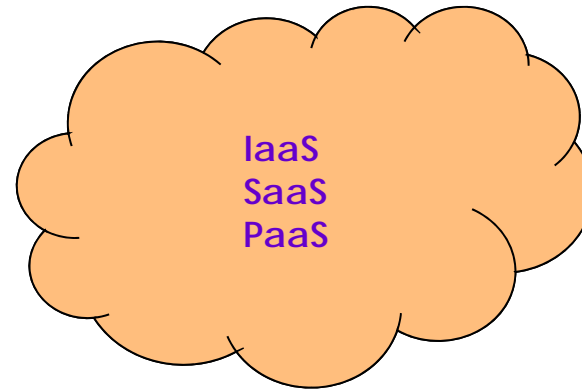
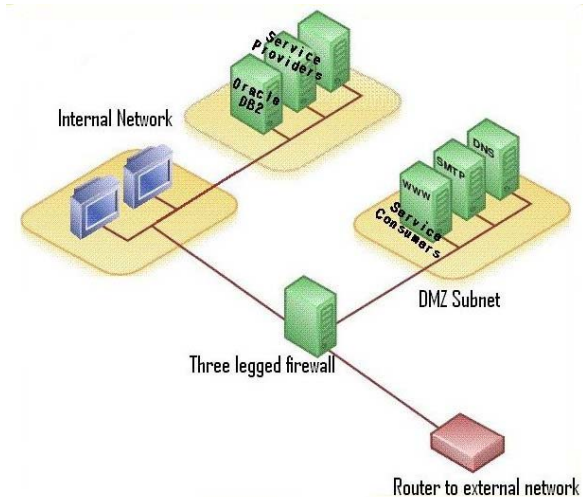
NCC Group



Why is this an issue?

- Blurring boundaries, more open networks for cost savings and business improvement
- Increasingly complex connectivity
- Trust placed in hands of suppliers
- Ultimately leads to loss of control of information

Why is this an issue?



Call centres
Outsourced processes
Advisors
Supply chain partners
etc

Why is this an issue?

- Verizon's 2009 Data Breach Investigation report shows 32% of breaches implicate partners and 30% involve multiple parties
- You can outsource the process... but you cannot outsource ownership of the risk...

Why is this an issue?



The screenshot shows the SC Magazine website interface. At the top, there is a navigation menu with categories like HOME, NEWS, PRODUCTS, ALERTS, STATS, BLOGS, WHITEPAPERS, and EVENTS. Below the menu, there are sub-categories such as Vulnerabilities & Exploits, Breaches & Exposures, Messaging, Mobile, Access Control, Biometrics & Forensics, and Legal. The main content area features a news article titled "Mozilla Store users suffer data breach" by Phil Muncaster, dated August 7, 2009. The article includes a sub-header "Change user names and passwords immediately." and a photograph of a padlock. To the left of the article is a sidebar with "Vulnerability Alerts" and "SANS" sections. To the right, there is a "RELATED ARTICLES" section and a "MOST F" section. The SC Magazine logo is visible in the top left corner, and a newsletter sign-up banner is at the top right.

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Sign up for the CRN newsletter for exclusive content

ie to help combat identity theft ▶ Cisco snaps up ScanSafe for \$200m

HOME NEWS PRODUCTS ALERTS STATS BLOGS WHITEPAPERS EVENTS

Vulnerabilities & Exploits Breaches & Exposures Messaging Mobile Access Control Biometrics & Forensics Legal

SC Magazine Australia/NZ > News > Vulnerabilities & Exploits > Web > Mozilla Store users suffer data breach

Vulnerability Alerts

SANS

- Infocon: green
- Sniffing SSL: RFC 4366 and TLS Extensions, (Wed, Oct 28th)

Microsoft

- Microsoft Security Bulletin Summary for August 2009
- MS09-043 - Critical: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638) - Version:2.0

CERT/CC

- SA09-286B: Multiple Vulnerabilities Affect Adobe Reader and Acrobat
- SA09-286A: Microsoft Updates for Multiple Vulnerabilities

[view more](#)

WEB

Mozilla Store users suffer data breach

By Phil Muncaster
Aug 7, 2009 10:03 AM
Tags: mozilla | store | data | breach | customer | details | user | names | passwords

Change user names and passwords immediately.

Users of the Mozilla Store have been warned to change their log-in passwords and user names if they use the same credentials on multiple sites, after the online store was breached earlier this week.

The organisation said in a [blog post](#) that GatewayCDI, a third-party provider which runs the online store's back end, had suffered a breach.

"Once notified, we took the immediate preventative step of shutting down the

RELATED ARTICLES

- Network Solutions suffers crippling data breach
- Do you know where your user IDs and passwords are?
- Almost 100,000 student details compromised in University of Florida data breach
- Heartland incident provides opportunity to standardise data breach notification laws

MOST F

- Fake defir
- ISPs
- Facr rela;
- Pop
- NSV bani
- Onir



Why is this an issue?



The screenshot shows the top of a web page from 'The Register'. The logo is in white on a red background with the tagline 'Biting the hand that feeds IT'. Below the logo is a navigation menu with categories: Hardware, Software, Music & Media, Networks, Security, Public Sector, Business, Science, Odds & Sods, Financial News, Small Biz, IT Director, and Tech Panel. The main content area features a large dark blue rectangular placeholder. Below this are 'Print' and 'Alert' icons. The article title is 'Webhost hack wipes out data for 100,000 sites' with a sub-headline 'Vaserv suspects zero-day virtualization vuln'. The author is 'Dan Goodin in San Francisco' and the article is dated '8th June 2009 20:02 GMT'. The text describes a data breach at Vaserv.com involving a zero-day vulnerability in HyperVM.

The Register
Biting the hand that feeds IT

Hardware Software Music & Media Networks Security Public Sector Business Science Odds & Sods
Financial News Small Biz IT Director Tech Panel

Print Alert

Webhost hack wipes out data for 100,000 sites

Vaserv suspects zero-day virtualization vuln

By [Dan Goodin in San Francisco](#) · [Get more from this author](#)

Posted in [Small Biz](#), 8th June 2009 20:02 GMT

[Free whitepaper – The VoIP journey](#)

A large internet service provider said data for as many as 100,000 websites was destroyed by attackers who targeted a zero-day vulnerability in a widely-used virtualization application.

Technicians at UK-based Vaserv.com were still scrambling to recover data on Monday evening UK time, more than 24 hours after unknown hackers were able to gain root access to the company's system, Rus Foster, the company's director told *The Register*. He said the attackers were able to penetrate his servers by exploiting a critical vulnerability in HyperVM, a virtualization application made by a company called [LXLabs](#).

"We were hit by a zero-day exploit" in version 2.0.7992 of the application, he said. "I've heard from other people they've been hit by the same thing."

Foster said he's been unable to reach anyone at LXLabs to discuss the suspected vulnerability. *The Register* has also received no response to inquiries sent to the company, which according to its website is located in Bangalore.



What is being done?

- Government - Connected for Health, SPF, CoCo. Standardising the way security is being requested from internal and external partners
- Corporate world - no such central control unfortunately
- Organisations have their own idea as to security requirements
- Leading to many (often complex) requests from multiple clients

What is being done?



Customer 1



Customer 2



Customer 3



Customer 4



Customer 5



Supplier a



Supplier b



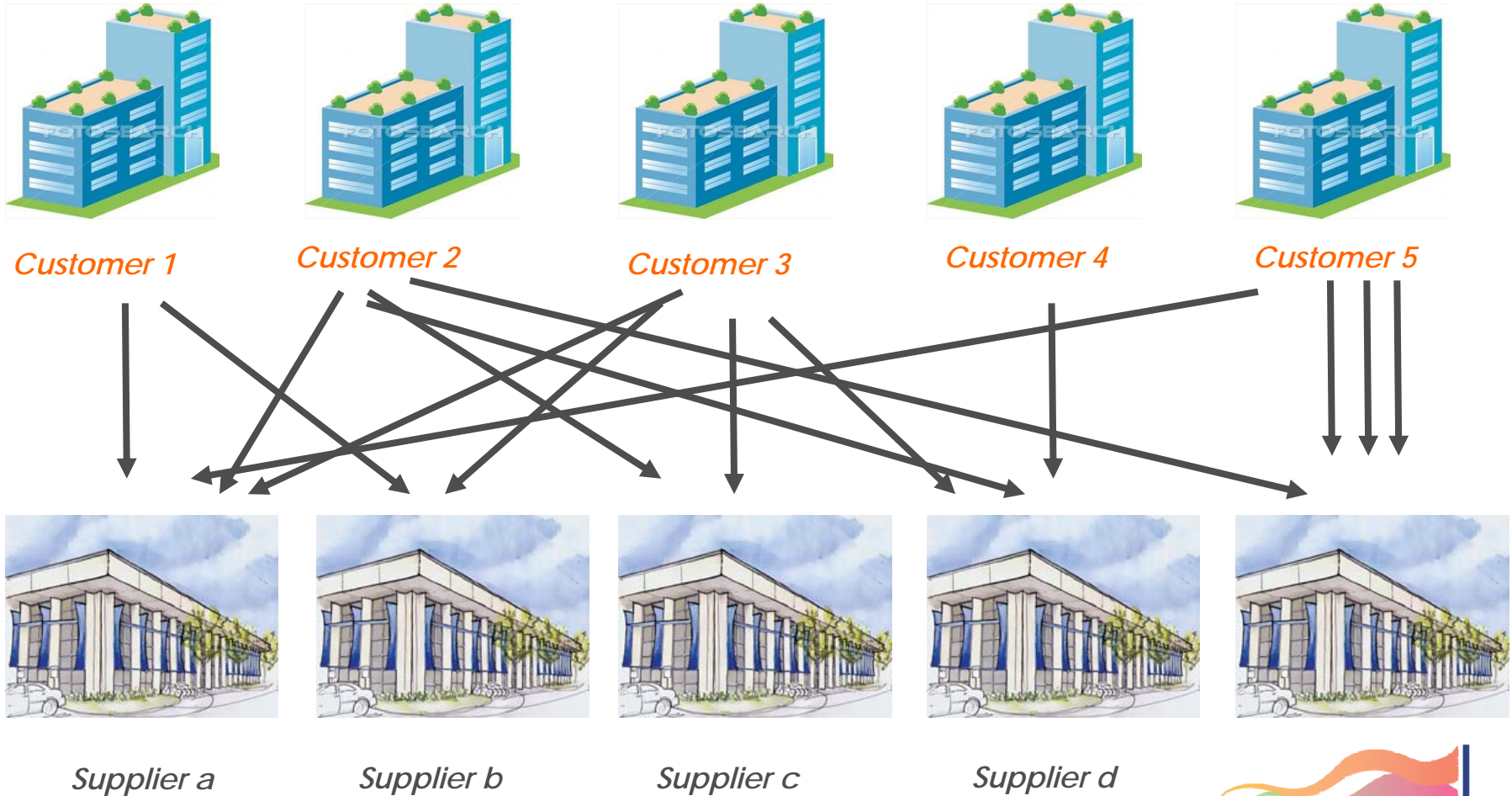
Supplier c



Supplier d



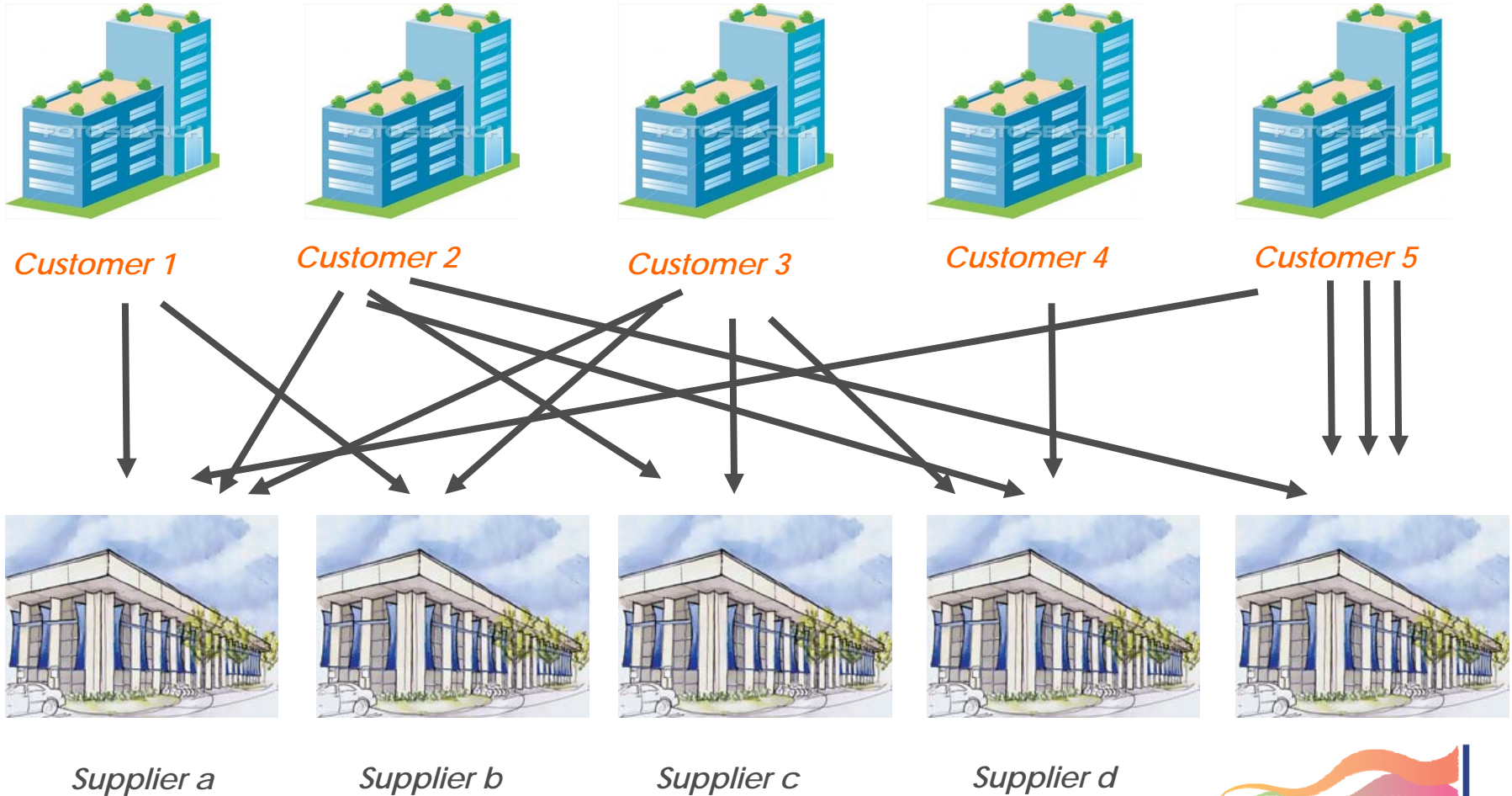
What is being done?



What is the answer?

- Is this enough?
- Pen testing? Yes, partially. Although difficulty in identifying the scope, and is this really enough?
- Audits
- Contractual relationships
- ISO27001? Impossible to enforce company wide, again, difficulty in identifying the scope

What is being done?



What is being done?



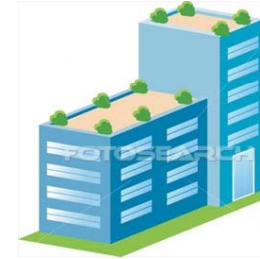
Customer 1



Customer 2



Customer 3



Customer 4



Customer 5

What are you doing?



Supplier a



Supplier b



Supplier c



Supplier d



A potential solution?



Customer 1



Customer 2



Customer 3



Customer 4



Customer 5



Independent certification based on:
Pen testing
Vulnerability monitoring
Review of policy and procedures



Supplier a



Supplier b



Supplier c



Supplier d

