TECH Tactics

A how-to guide to improving business technology

BY DAVE VAGNONI

STEPS TO SUCCESS

Strengthen Data Security

It wasn't until late March of 2007 – about two years after the breach first occurred – when the truth came out. TJX Companies, which operates T.J.Maxx, Marshalls and HomeGoods, admitted that more than 45 million customer credit and debit card numbers were stolen by hackers. It was the biggest data breach in history, and it was made possible simply because a wireless network was left unsecured. "By now, the message should be clear: Companies that collect sensitive consumer information have a responsibility to keep it secure," said then-FTC Chairman Deborah Platt Majoras, following the incident.

While your company may not rival the size of TJX, the lessons from its case are important for every business. Pleading ignorance is no excuse, and liability can't be brushed off to a third party. Even a minor breach can lead to lawsuits, extensive repair costs and a customer base that goes elsewhere. "You need to monitor your reputation," says Gary Bahadur, CEO of KRAA Security. "A bad reputation can kill a business."

Improving data security requires the commitment of everyone involved in your company. While good anti-virus software can help protect sensitive information, there are several other measures that can further close gaps in your coverage. Here are six steps to take.

STEP #1
Identify Sensitive Information

Experts recommend companies take an inventory of their data to figure out vulnerabilities. "You need to do an initial assessment and understand foreseeable threats," says Lynn Holdsworth, a MA-based information security expert. Pay special attention to where you store your bank statements and account information, customers' credit card and social security numbers, and files you tend to transfer through cloud computing. An internal network administrator or IT manager can spearhead this tracking process, but a team of senior leaders should also be involved.

STEP #2
Develop Employee Policies

A lack of data security rules can easily compromise information. In fact, a recent study released by Cisco Systems shows 70% of IT professionals believe the use of unauthorized programs led to half of their companies' data loss incidents. To combat the trend, use network permissions to limit the number of employees who have access to critical data. Remind employees not to share passwords with coworkers and not to transfer sensitive files when working from home. Also, warn staff members against opening personal e-mail attachments in the office. "Make policies clear and provide training," says Ken Leeser, president of Kaliber Data Security. "Put in place penalties as well."

STEP #3
Focus On Encryption, Passwords & Updates

Adding digital locks can make an instant impact on data security. All important information needs to be encrypted – a fancy way of saying unreadable. TrueCrypt, PGP and Vix are all considered good encryption software programs. At a minimum, you should also use passwords for desktop computers, laptops and mobile devices. A strong password contains 10 characters, with a mix of uppercase and lowercase letters, numbers and other symbols. Anti-virus software like Norton, AVG or Kaspersky is also a necessity. Security updates and patches are critical to data protection as well. "It's really about computer hygiene," says Andrew Wild, chief security officer for risk management firm Qualys. "In a lot of cases, vulnerabilities were fixed in software devices years ago, but companies just don't install the updates."

EXCLUSIVE VIDEO:
Want even more data security tips? Go to *www.CounselorMag.com* to check out our latest Tech Tactics video.

TIP: Use an encrypted USB stick to back up data. You can buy a 16 GB flash drive for under $50.

STEP #4
Remember Mobile Technology & Social Media

With the expansion of mobile devices – from smartphones to tablets to laptops – experts say companies can't afford to ignore the potential for data exposure. Besides locking your device with a passcode, you should also install virus protection and be able to disable your mobile equipment remotely. Be cautious in downloading mobile apps, especially if they're in the Android marketplace, which is generally viewed by experts as less secure than the iPhone App Store. Finally, don't be lulled into thinking popular social networks and blogs are always safe. "Viruses can be spread through Facebook and Twitter," says John Williams, founder of consultancy FMP Companies. "I'm highly concerned with social media."

STEP #5
Choose Good Partners

Before you hire any vendor to either host your data on the cloud or provide e-commerce services for your website, you need to be sure you're working with a reputable company. Ask for PCI compliance documentation (required by major credit card companies) and other security protocols upfront. "Read the fine print," says Trey Wilkins, owner of Georgia-based Wilkins Consulting. "If a provider is local, tour its facility and make a comprehensive list of security measures like cameras and biometric entry into data centers."

STEP #6
Create A Breach Response Plan

If a data breach does occur at your firm, experts say you have to take measured action to prevent further information loss. "You need to have strategy in place," says Bahadur of KRAA. "A breach isn't just the marketing department's problem." First, a business continuity plan is a must. Staff members should have pre-assigned responsibilities for on-site and off-site recovery. When data leakage could result in harm to a person or business, you must call your local police department immediately. Banks, credit reporting agencies and affected individuals may have to be contacted as well, depending upon what a breach investigation reveals.

Q&A
Safe & Sound

Counselor asked Sari Greene, president of Sage Data Security, for advice on protecting sensitive information.

Q What can a business owner do immediately to keep hackers away?

A Do not store (digitally or hard copy) any more information than necessary. Don't forget the basics – strong passwords, anti-virus software, OS and application security patching, firewall rules and encrypted wireless. Never respond to unsolicited requests for information. Do not click on embedded links in e-mail.

Q What's the cost involved in making sure a website is secure?

A It depends upon the functionality and design of the website. Discuss security upfront with designers and require security testing prior to productions. Recognize that website changes can introduce new vulnerabilities.

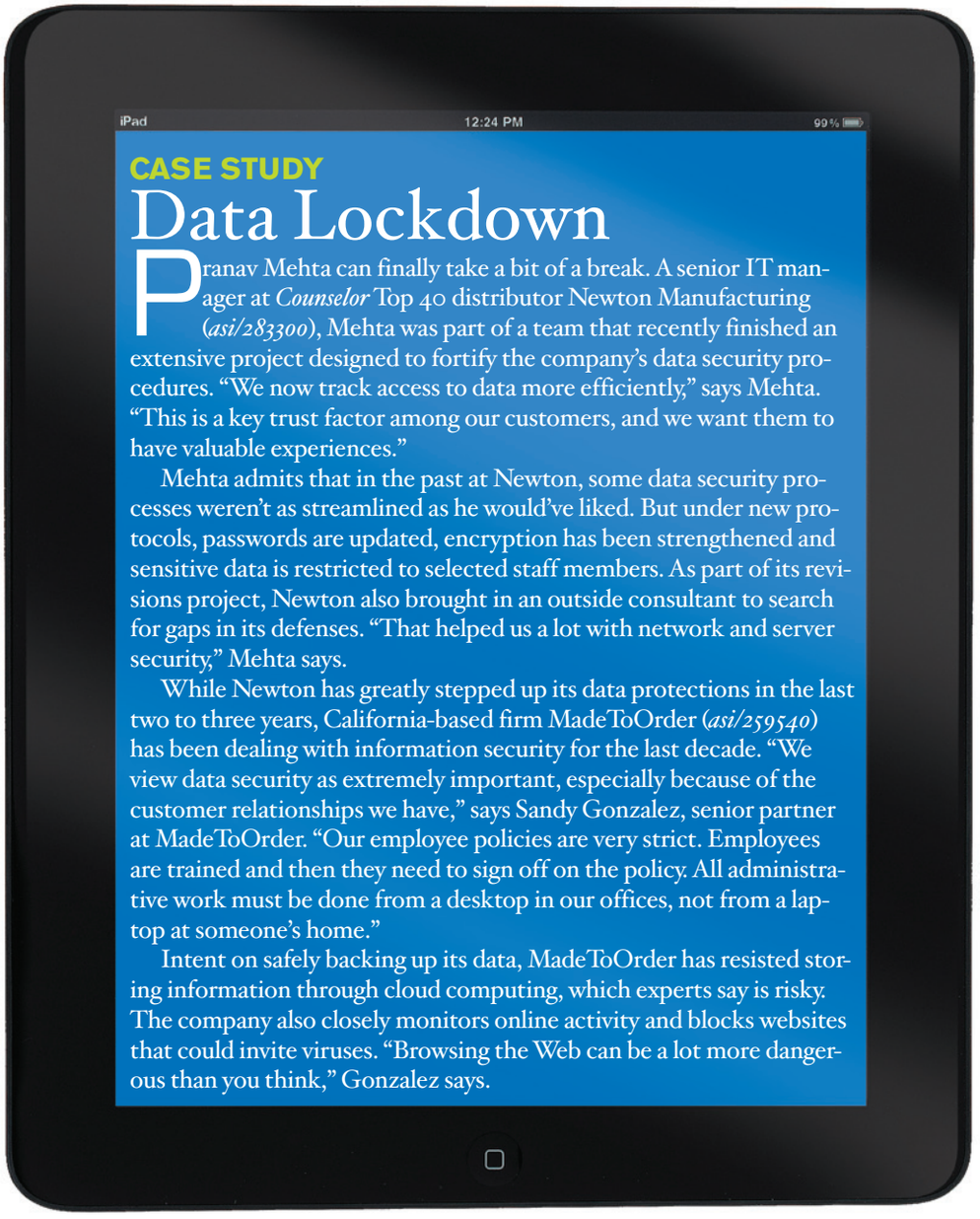
Q What are the greatest data security threats that exist right now?

A Without a doubt, it's malware. Be especially aware of Trojan Zeus and Spy Eye. Also, corporate account takeovers. Small businesses that engage in online banking transfers such as ACH and wire should be aware that there are no regulations that protect commercial accounts. If their credentials are compromised and fraudulent activity ensues, their bank has no obligation to make them whole.

Q Are there dangers in social media and cloud computing?

A Social media is widely used to infiltrate companies, so only associate with those you know. Confidential data should not be placed in a computing cloud where a user gives up control of information to a security provider.

TECH Tactics



CASE STUDY

Data Lockdown

Pranav Mehta can finally take a bit of a break. A senior IT manager at *Counselor* Top 40 distributor Newton Manufacturing (*asi/283300*), Mehta was part of a team that recently finished an extensive project designed to fortify the company's data security procedures. "We now track access to data more efficiently," says Mehta. "This is a key trust factor among our customers, and we want them to have valuable experiences."

Mehta admits that in the past at Newton, some data security processes weren't as streamlined as he would've liked. But under new protocols, passwords are updated, encryption has been strengthened and sensitive data is restricted to selected staff members. As part of its revisions project, Newton also brought in an outside consultant to search for gaps in its defenses. "That helped us a lot with network and server security," Mehta says.

While Newton has greatly stepped up its data protections in the last two to three years, California-based firm MadeToOrder (*asi/259540*) has been dealing with information security for the last decade. "We view data security as extremely important, especially because of the customer relationships we have," says Sandy Gonzalez, senior partner at MadeToOrder. "Our employee policies are very strict. Employees are trained and then they need to sign off on the policy. All administrative work must be done from a desktop in our offices, not from a laptop at someone's home."

Intent on safely backing up its data, MadeToOrder has resisted storing information through cloud computing, which experts say is risky. The company also closely monitors online activity and blocks websites that could invite viruses. "Browsing the Web can be a lot more dangerous than you think," Gonzalez says.

TECH TALK

Facebook responses to our question: **What online site do you shop on the most?**

Jen Brun
Amazon, of course.

Ryan Schade
Amazon.

Ted Pendlebury
Slickdeals, via RSS feed.

Jennifer Valanski Moyer
Amazon.

Justin Graham
Amazon, because of Prime. Slickdeals is awesome, though!

Bonnie Landsberger
Amazon.com and TigerDirect.com.

CHAT WITH US

Be Part Of The Online Conversation

Have questions? Want to share ideas or advice? Join us for an online chat about strengthening data security on Tuesday, December 13 at 2:00 p.m ET. Go to *www.asicentral.com/counselorchat* to take part in the live discussion, moderated by *Counselor* Senior Writer Dave Vagnoni.