CCC News

Control Computer Crimes
Issue 0010 - 15 November 2009

Message from the Editor

Welcome to the tenth issue of CCCNews Magazine.

In this edition, we bring you a handful of interesting and educational reports, analysis and research.

One of the big attractions in this issue is a research report on – "Why Security Matters Now". This provides an insight and detailed analysis of security requirements and trends and what we need to do about these.

Another interesting research analysis is on how computers can do wrong mathematics. The wrong calculations may lead to catastrophes like wrong firing of missile or rocket can be exploded in mid-flight or death of patient in a hospital.

Another interesting analytic story describe that how a PC virus in your computer can assist a criminal to store porn and illegal contents on your computer, thus making you liable for legal action against you. Be Beware.

Further, we bring to you the details on how computer criminals mix sophisticated Trojans and Money mules to defraud the normal users and money mule using state-of-the-art technique.

A research shows that more and more people are adding Information Security to their careers options, finding it most lucrative career options amongst all. We bring a report on this research for you.

We also bring to you an educational article on how to avoid five email mistakes, which can be detrimental to your business interests.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0010
15 November 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

LAST ISSUE DOWNLOAD COUNT : 160,000+

RESEARCH

Computers Can Do Wrong Maths

How simple calculations can be a matter of life and death

Computers might struggle to exhibit intelligent behaviour, but blindly performing arithmetic calculations is surely their forte. Or is it?

The failure of Google's online calculator and Excel's apparent inability to give correct answers to simple calculations are both well-known problems among programmers, but these aren't really bugs in the normal sense of the word. Instead they're just a consequence of the fact that computers suck at maths.

Computers perform calculations in quite a different way from the methods that humans use to do arithmetic – and that means that they habitually come up with the wrong answer. Here we investigate some of the shocking consequences of this revelation before delving into the reason why computers suck at maths.

Close isn't close enough

For anyone still to be convinced that computers can't get simple arithmetic right, let's start off with a few examples that you can try out yourself.

First up, Google's calculator. If you've never tried it out before, to get a feel for how it works, surf to www.google.co.uk, type 5*9+(sqrt 9)^3 into the search box and click on 'Search'. You'll find that it comes back with the correct answer: '5 * 9 + (sqrt 9) ^3 = 72'.

Now let's try another calculation. Type in 599,999,999,999,999 - 599,999,999,999,998. Quite clearly, this should give an answer of 1. Unbelievably, however, Google responds with this: '599,999,999,999,999 – 599,999,999,999,998 = 0'. Just a rare and unfortunate example, perhaps?

OK then, let's try another simple calculation. Type =850*77.1 into cell A1 of an Excel 2007 workbook (it doesn't work – or should that be it does work – in earlier versions of Excel). A bit of mental arithmetic suggests that the answer ought to be in the region of 60,000; in fact the correct answer is 65,535.

Excel has other ideas. It will tell you that the result of this multiplication is 100,000, which is out by a massive 34,465. And to prove that this is no flash in the pan, how about using a selection of online calculators to work out 1.0 - 0.9 - 0.1?

You'll probably find at least half of them will come up with an answer of -2.77555756 E-17 – scientific notation for -0.0000000000000000277555756. (If all the ones you try give the right answer, take a look at www.calculator.net.)

OK, this answer might not be far removed from the correct answer of 0, but why can't the calculator come up with the right answer – an answer that's blatantly obvious to anyone who is conversant with simple arithmetic?

How computers do maths

Although computers can handle integers (whole numbers), for general-purpose arithmetic they store numbers in floating point format because it's so much more efficient in memory use.

Let's take the double precision floating point representation as an example. It uses 64 bits to store each number and permits values from about -10308 to 10308 (minus and plus 1 followed by 308 zeros, respectively) to be stored. Furthermore, fractional values as small as plus or minus 10-308 (that's a decimal point followed by 307 zeros and then a 1) can be stored.

By way of contrast, if the same 64 bits were used to store integers, the range would be −9,223,372,036,854,775,808 to +9,223,372,036,854,775,807, and fractional values couldn't be represented.

The secret to this apparently amazing efficiency is approximation. Of those 64 bits, one represents the sign (so whether the value is positive or negative), 52 bits represent the mantissa (that's the actual numbers) and the remaining 11 bits represent the exponent (how many zeros there are or where the decimal point is).

So although a much greater range of numbers can be stored using floating point notation, the precision is actually less than can be achieved in integer format, since only 52 bits are available. In fact, 52 bits of binary information represents a 16-bit decimal number, so any values that differ only in their 17th decimal point will actually be seen as identical.

The situation with Google thinking that 599,999,999,999,999 - 599,999,999,999,998 equals 0 is similar, although it's evident that

Google's calculator actually uses less than the normal 52 bits for the mantissa. That some calculators give a non-zero result to the calculation 1.0 - 0.9 - 0.1 might seem different since we appear to be nowhere close to the limit of 64-bit floating point arithmetic.

But that's forgetting one important fact – that computers work in binary. And although 0.1 might have only one significant digit in decimal, in binary notation the mantissa is a repeating sequence. This means that 0.1 can never be represented accurately in binary, no matter how many bits you use.

The discrepancy between the computed answer and the correct answer is often minute, and you might be inclined to dismiss this sort of error as insignificant. However, such errors can add up, and the consequences can be serious.

On 25 February 1991, three days before the end of the first Gulf War, an Iraqi Scud missile hit a US airfield in Dhahran, Saudi Arabia. 28 American soldiers were killed and more than 100 others were injured.

At the time, sensitive targets were supposed to be protected by the Patriot surface-to-air defence system, and one battery of Patriot missiles was assigned to the Dhahran facility – so it's pertinent to ask what exactly went wrong.

The answer is the system's tracking software, and the problem is not unrelated to our online calculator error. In order to avoid potentially costly false alarms, the Patriot's sophisticated radar must first detect an object that has the characteristics of a Scud missile and then detect it a second time in a position calculated by the system on the assumption that the first fix was genuinely a Scud. Only when this second fix provides a confirmation is a missile launched to intercept it.

The calculation of where to look for confirmation of an incoming missile requires knowledge of the system time, which is stored as the number of 0.1-second ticks since the system was started up. Unfortunately, 0.1 seconds cannot be expressed accurately as a binary number, so when it's shoehorned into a 24-bit register – as used in the Patriot system – it's out by a tiny amount. But all these tiny amounts add up.

At the time of the missile attack, the system had been running for about 100 hours, or 3,600,000 ticks to be more specific. Multiplying this count by the tiny error led to a total error of 0.3433 seconds, during which time the Scud missile would cover 687m.

The radar looked in the wrong place to receive a confirmation and saw no target. Accordingly no missile was launched to intercept the incoming Scud – and 28 people paid with their lives.

The processor that couldn't divide

Launched in March 1993, the Pentium was Intel's fifth generation of x86 processor. Unlike previous generations, in which at least some family members could only carry out arithmetic on whole numbers, all Pentiums had a floating point unit (FPU).

An FPU is a piece of built-in hardware for calculating floating point arithmetic. This gave the Pentium a massive speed advantage, since computers without an FPU-enabled processor had to carry out this sort of calculation using software routines that involved lots of integer operations. Unfortunately, it was a poisoned chalice for Intel.

In June 1994, shortly after taking delivery of a Pentium-based PC, Thomas Nicely – then Professor of Mathematics at Lynchburg College, Virginia – noticed that a program he had written was giving inconsistent results.

By running the same program on several machines, Professor Nicely tracked down the problem to the his new PC's Pentium processor and, in particular, to its FDIV (floating point division) instruction. Although it affected just a tiny proportion of floating point divisions, at its worst the error was really quite significant.

Dividing 4,195,835 by 3,145,727 gave an answer of 1.3337 – which represents an error in the fourth decimal place since the correct answer is actually 1.3338. The Pentium's FPU used something called the SRT algorithm to carry out floating point divisions.

Although there are simpler and more obvious ways of dividing one floating point number by another, the SRT algorithm gave a significant speed advantage over previous algorithms.

If you're not a mathematician you'll find a description of how SRT works totally impenetrable. However, let's just say that instead of working everything out using 'pure maths', it involved the use of a look-up table. The table contained 1,000 or so values, but due to a production error five of these values were missing.

Despite the fact that Intel's CEO Andy Grove reckoned that the average user would only see the problem every 27,000 years, IBM's estimate was once every 24 days – and as a result the company stopped shipping Pentium-based PCs. Intel eventually agreed to swap defective Pentiums for good ones.

Most people didn't take up the offer, but the delay caused technically minded users to make Intel the butt of their jokes. The following is typical. Q: How many Pentium designers does it take to change a light bulb? A: 1.99904274017, but that's close enough for non-technical people.

The errors we've seen so far have concerned floating point numbers where accuracy is lost if there's not enough bits to store the mantissa. OK, those errors can add up, but essentially they're just rounding errors, and the likelihood of not having enough bits to store the exponent is comparatively small given that the maximum values they can store are absolutely huge.

When integers are involved, the effect can actually be far more serious. A 64-bit integer can store a maximum positive value of 9,223,372,036,854,775,807. If you try adding 1 to an integer variable that already equals this maximum value, you don't just lose that extra value. Instead, the integer overflows.

In other words, as far as a computer working in 64-bit integer arithmetic is concerned, 9,223,372,036,854,775,807 + 1 = -9,223,372,036,854,775,808 (note the minus sign). Something very similar happened on-board the European Space Agency's Ariane V rocket on its maiden flight.

In fact, the arithmetic operation in question – if you can call it that – was even simpler than adding 1. Instead, it just involved copying one number that had been stored in floating point format to another location that was defined as an integer – and a 16-bit integer at that (maximum positive value of 32,767).

Unfortunately, the number was already too large to fit in the integer location, and as a result it overflowed. The exact sequence of events that followed is pretty complex but, to cut a long story short, the end result was that the Ariane V became one of the most expensive fireworks in history.

Guarding against cock-ups

This run-through of some of computing's most astonishing mathematical cock-ups may have come as something of an eye-opener to you. If so, you're probably wondering whether tomorrow's computers can avoid making such elementary mistakes.

Surprisingly, perhaps – and with the exception of the Pentium floating point error, which was caused by a hardware glitch – all of the errors we've mentioned here could have been prevented. In that sense, they can all be thought of as software errors.

As an example, let's take that integer overflow on the Ariane V rocket. That an integer can overflow isn't an error on the part of the processor because it's the way it's supposed to work. But whenever an integer does overflow, the processor sets something called a flag that the program can interrogate.

In the case of the Ariane software, the program didn't check for an overflow; if it had done, corrective action could have been taken. Of course, there will always be a limit to how large an integer can be and how much precision a floating point number can have – and this depends on the processor. But all of today's computers are universal computing machines, which means that they can solve any problem involving logic and maths.

So if a processor's internal instructions can't operate on large enough integers or on floating point numbers with sufficient precision, it's always possible for the programmer to implement arithmetic routines that will.

There will be a trade off against speed, though, which is why this isn't usually done. However clever the software or however much memory you use to store a floating point number, the result of some divisions will never be accurate.

We've seen how 1 divided by 10 is an infinite string in binary, and, in the general case, a move to decimal arithmetic wouldn't help either: 1 divided by 10 can be stored accurately in decimal, but 1 divided by 3 equals 0.3333333… ad infinitum.

The bottom line is that whatever number base you choose, some divisions will produce results that can never be stored accurately as a finite number of digits. Even this isn't a show-stopper, though.

Remember how 1.0 - 0.9 - 0.1 often yields an inaccurate answer because of rounding errors even though we know, immediately, that the answer is 0? Well, it's quite possible to write software to store the result of a division as a rational number.

In other words, you don't actually do the division – you just store the two numbers. In subsequent arithmetic operations you handle the values as fractions, just as you were taught in school, and the result will be exact.

So computers might suck at maths, but there's always a solution available to circumvent their inherent weaknesses. And in that case, it's probably more accurate to say that computer programmers suck at maths – or at least some of them do.

Courtesy : Mike Bedford; www.techradar.com
29 Oct 2009

ANALYSIS

Cyber Criminals Mix Sophisticated Trojans and Money Mules to Hack Bank Accounts

According to Internet security experts, there are high possibilities that cyber criminals would mix Trojan viruses with money mules (a sophisticated combination) in future to hack bank accounts.

Yuval Ben-Itzhak, Chief Technology Officer at Finjan, said - the above mentioned technique would be possible because cyber criminals always attempted to grab money from bank accounts through creative means, as reported by SENTOR on October 5, 2009.

Ben-Itzhak said that a competition always existed between Internet crooks and banks in which both parties tried to enhance their mechanisms for accomplishing their respective objectives that might involve financial institutions looking for avoiding a security breach.

He further said that it was certain cyber criminals would improve their methods from what experts had observed in recent years, adding that he himself saw no reason why they would stop.

Ben-Itzhak's remarks follow Garlik's 3rd annual British Cyber-crime report, which disclosed that online crooks were responsible for over 3.6 Million illegal operations on the Net in 2008 as they adjusted their schemes according to the economic and social changes in the Great Britain.

There was a constant challenge in front of banks that they should check the veracity of each transaction, said Ben-Itzhak. Thus, they had to ensure that all security arrangements were in place at institutions so that the crooks could be prevented from breaking in.

Moreover, the expert's advice comes after reports that Internet crooks have been employing fresh methods for hacking into Web users' financial accounts, including debit and credit card accounts. The Malicious Code Research Center of Finjan states that criminals design these methods in such a way that detection might be minimal.

Cyber criminals use modern malware that gives a completely new form to hacking. Recently, Finjan found a novel strain of malicious program, which concealed clues of diminishing bank balance of an accountholder via the overwriting of his bank statement.

The technique gave enough time to the criminals to commit fraud prior to victim realizing his situation. Nevertheless, the hack would have failed if the victim had examined his bank balance from an uninfected computer, the company stated.

Courtesy : SPAMfighter News; www.spamfighter.com
27-10-2009

SUREVY

Why Security Matters Now

Today's most compelling technologies are giving you the biggest security headaches. Social networking sites such as Twitter, Facebook and LinkedIn enhance collaboration and help your company connect with customers, but they also make it easier than ever for your employees to share customer data and company secrets with outsiders.

Virtualization and cloud computing let you simplify your physical IT infrastructure and cut overhead costs, but you've only just begun to see the security risks involved. Putting more of your infrastructure in the cloud has left you vulnerable to hackers who have redoubled efforts to launch denial-of-service attacks against the likes of Google, Yahoo and other Internet-based service providers. A massive Google outage earlier this year illustrates the kind of disruptions cloud-dependent businesses can suffer.

But there's also good news. Even though the worst economic recession in decades has compelled you to spend less on outsourced security services and do more in-house, your security budget is holding steady. And more of you are employing a chief security officer.

Such are the big takeaways from the seventh-annual Global Information Security survey, which CIO and CSO magazines conducted with PricewaterhouseCoopers earlier this year. Nearly 7,300 business and technology executives worldwide responded from a variety of industries, including government, health care, financial services and retail.

These trends are shaping your information security agenda. "Every company worries about protecting their data, especially their client data," says Charles Beard, CIO at Science Applications International Corp. (SAIC). "Under the old business model, everyone had to get together in the same building in the same geographical area. Now everyone is using the Internet and mobile devices to work with each other. That's where we see the promise of things like social networking. The flip side is we're exposed to the dark side of cyberspace. Adoption of this technology is well ahead of efforts to properly secure and govern it."

Top IT Security Priorities

New investments are focused on protecting data, authenticating users

1. Biometrics
2. Web content filters
3. Data leakage prevention
4. Disposable passwords/smart cards/tokens
5. Reduced or single-sign-on software
6. Voice-over-IP security
7. Web 2.0 security
8. Identity management
9. Encryption of removable media

TREND #1

The Promise and Peril of Social Networking

In less than two years, social networking has gone from an abstract curiosity to a way of life for many people. When someone updates their status on Twitter, Facebook or LinkedIn, they might do it at work by day or on company-owned laptops from home at night.

What gives IT executives heartburn is the ease with which users could share customer data or sensitive company activities while they're telling you what they're having for lunch. Cyberoutlaws know this and use social networks to launch phishing scams. In one popular attack, they send their victims messages that appear to be coming from a Facebook friend. The "friend" may send along a URL they insist you check out. It may be pitched as a news story about Michael Jackson's death or a list of stock tips. In reality, the link takes the victim to a shady website that automatically drops malware onto the computer. The malware goes off in search of any valuable data stored on the computer or wider company network, be it customer credit card numbers or the secret recipe for a new cancer-fighting drug.

It's no surprise, then, that every IT leader surveyed admitted they fear social-engineering-based attacks. Forty-five percent specifically fear the phishing schemes against Web 2.0 applications.

Nevertheless, for many company executives, blocking social networking is out of the question because of its potential business benefits. Companies now clamor to get their messages out through these sites, so the challenge for CIOs is to find the right balance between security and usability.

"People are still incredibly naïve about how much they should share with others, and we have to do a better job educating them about what is and isn't appropriate to share," says H. Frank Cervone, vice chancellor of information services with Purdue University Calumet. "We have to do a better job of enhancing our understanding of what internal organization information should not be shared."

But in a university setting, it's critical to engage people through social media, Cervone adds. Even in the commercial sector, he doesn't see how organizations can avoid it.

And yet this year--the first in which we asked respondents about social media, only 23 percent said their security efforts now include provisions to defend Web 2.0 technologies and control what can be posted on social networking sites. One positive sign: Every year, more companies dedicate staff to monitoring how employees use online assets--57 percent this year compared to 50 percent last year and 40 percent in 2006. Thirty-six percent of respondents monitor what employees are posting to external blogs and social networking sites.

To prevent sensitive information from escaping, 65 percent of companies use Web content filters to keep data behind the firewall, and 62 percent make sure they are using the most secure version of whichever browser they choose. Forty percent said that when they evaluate security products, support and compatibility for Web 2.0 is essential.

Unfortunately, social networking insecurity isn't something one can fix with just technology, says Mark Lobel, a partner in the security practice at PricewaterhouseCoopers.

"The problems are cultural, not technological. How do you educate people to use these sites intelligently?" he asks. "Historically, security people have come up from the tech path, not the sociologist path. So we have a long way to go in finding the right security balance."

Guy Pace, security administrator with the Washington State Board for Community and Technical Colleges, says his organization takes many of the precautions described above. But he agrees with Lobel that the true battleground is one of office culture, not technology. "The most effective mitigation here is user education and creative, effective security awareness programs," he says.

TREND #2

Jumping into the Cloud, Sans Parachute

Given the expense to maintain a physical IT infrastructure, the thought of replacing server rooms and haphazardly configured appliances with cloud services is simply too hard for many companies to resist. But rushing into the cloud without a security strategy is a recipe for risk.

According to the survey, 43 percent of respondents are using cloud services such as software as a service or infrastructure as a service. Even more are investing in the virtualization technology that helps to enable cloud computing. Sixty-seven percent of respondents say they now use server, storage and other forms of IT asset virtualization. Among them, 48 percent actually believe their information security has improved, while 42 percent say their security is at about the same level. Only 10 percent say virtualization has created more security holes.

Dark Cloud

Fears about vendors dominate cloud security risks.
What is the greatest security risk to your cloud computing strategy?

- Ability to enforce provider security policies: 23%
- Inadequate training and IT auditing: 22%
- Access control at provider site: 14%
- Ability to recover data: 12%
- Ability to audit provider: 11%
- Proximity of company data to someone else's: 10%
- Continued existence of provider: 4%
- Provider regulatory compliance: 4%

Security may well have improved for some, but experts like Chris Hoff, director of cloud and virtualization solutions at Cisco Systems, believe that both consumers and providers need to ensure they understand the risks associated with the technical, operational and organizational changes these technologies bring to bear.

"When you look at how people think of virtualization and what it means, the definition of virtualization is either very narrow--that it's about server consolidation, virtualizing your applications and operating systems, and consolidating everything down to fewer physical boxes--or it's about any number of other elements: client-side desktops, storage, networks, security," he says. "Then you add to the confusion with the concept of cloud computing, which is being pushed by Microsoft and a number of smaller, emerging companies. You're left scratching your head wondering what this means to you as a company. How does it impact your infrastructure?"

Fortunately, there's some evidence of companies proceeding with caution. One example is Atmos Energy, which is using Salesforce.com to speed its response time to customers and help the marketing department manage a growing pool of clients, according to CIO Rich Gius.

The endeavor is successful thus far, so Gius is investigating the viability of running company e-mail in the cloud. "It would help us address the growing challenge where e-mail-enabled mobile devices like BlackBerrys are proliferating widely among the workforce," he says. But he's not ready to take such a big step because the risks, including security, remain hard to pin down. One example of the disruption that cloud-dependent companies can experience came in May, when search giant Google--whose content accounts for 5 percent of all Internet traffic--suffered a massive outage. When it went down, many companies that have come to rely on its cloud-based business applications (such as e-mail) were dead in the water.

The outage wasn't caused by hackers, but there are signs that cybercriminals are exploring ways to exploit the cloud for malicious purposes. On the heels of the outage, attackers added insult to injury by flooding Google search results with malicious links, prompting the U.S. Computer Emergency Response Team (U.S. CERT) to issue a warning about potential dangers to cloud-based service sites.

The attack poisoned several thousand legitimate websites by exploiting known flaws in Adobe software to install a malicious program on victims' machines, U.S. CERT says. The program would then steal FTP login credentials from victims and use the information to spread itself further. It also hijacked the victim's browser, replacing Google search results with links chosen by the attackers. Although the victimized sites were not specifically those offering cloud-based services, similar schemes could be directed at cloud services providers.

IT organizations often make an attacker's job easier by configuring physical and cloud-based IT assets so poorly that easy-to-find-and-exploit flaws are left behind. Asked about the potential vulnerabilities in their virtualized environments, 36 percent cited misconfiguration and poor implementation, and 51 percent cited a lack of adequately trained IT staff (whose lack of knowledge leads to configuration glitches). In fact, 22 percent of respondents cited inadequate training, along with insufficient auditing (to uncover vulnerabilities) to be the greatest security risk to their company's cloud computing strategy.

It's this awareness that makes Atmos Energy's Gius proceed with caution. "We have no CSO. If we were a financial services firm it might be a different story, or if we had a huge head count," Gius says. "But we are a small-to-medium-sized company, and the staff limitations make these kinds of implementations more difficult."

Even with the right resources, security in the cloud is a matter of managing a variety of risks across multiple platforms. There's no single cloud. Rather, "there are many clouds, they're not federated, they don't natively interoperate at the application layer and they're all mostly proprietary in their platform and operation," Hoff says. "The notion that we're all running out to put our content and apps in some common [and secure] repository on someone else's infrastructure is unrealistic."

Lobel, with PricewaterhouseCoopers, says perfect security is not possible. "You have to actively focus on the security controls while you are leaping to these services," he says. It's difficult for companies to turn back once they have let their data and applications loose because they are often quick to rid themselves of the hardware and skills they would need to bring the services back in-house.

"If you dive down a well without a rope, you may find the water you wanted, but you're not going to get out of the well without the rope," he says. "What if you have a breach and you need to leave the cloud? Can you get out if you have to?"

Trend #3

Insourcing Security Management

A few years ago, technology analysts were predicting unlimited growth for managed security service providers (MSSPs). Many companies then viewed security as a foreign concept, but laws such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act (affecting financial services) were forcing them to address intrusion defense, patch management, encryption and log management.

Data Dangers

Attacks on data have increased faster than any other security exploit. The top target: databases.

How Attackers Get Your Data

- Databases: 57%
- File-sharing applications: 46%
- Laptops: 39%
- Removable Media: 23%
- Backup Tapes: 16%

(Multiple Responses Allowed)

Convinced they couldn't do it on their own, companies chose outsourcers to do it for them. Gartner estimated the MSSP market in North America alone would reach $900 million in 2004 and that it would grow another 18 percent by 2008.

Then came the economic tsunami, which appears to have cast a shadow over outsourcing plans even though security budgets are holding steady. Although 31 percent of respondents this year are relying on outsiders to help them manage day-to-day security functions, only 18 percent said they plan to make security outsourcing a priority in the next 12 months.

When it comes to specific functions, the shift has already begun. Last year, 30 percent of respondents said they were outsourcing management of application firewalls, compared to 16 percent today. Respondents cited similar reductions in outsourcing of network and end-user firewalls. Companies have also cut back on outsourcing encryption management and patch management.

At the same time, more companies are spending money on these and other security functions. Sixty-nine percent said they're budgeting for application firewalls, up slightly compared to the past two years. Meanwhile, more than half of respondents said they are investing in encryption for laptops and other computing devices.

The results surprise Lobel of PricewaterhouseCoopers. "When you think about it logically, some IT organizations have the resources and maturity to manage their operating systems and patches, but many don't," he observes. "Hopefully, the numbers simply mean IT shops have grown more mature in their security understanding."

Security Budgets Hold Stead

More companies are increasing spending than cutting it.

Direction of Spending

- ❖ Increase: 38%
- ❖ Stay the Same: 25%
- ❖ Decrease: 12%
- ❖ Don't Know: 24%

(Numbers may not add up to 100% due to rounding)

Gius of Atmos Energy offered another possible explanation: Companies see a lot of chaos in the security market with an avalanche of mergers and acquisitions. One independent security vendor after another has merged with or been acquired by other companies. Examples include BT's acquisition of Counterpane and IBM's acquisition of Internet Security Systems. IT leaders are simply getting out of the way until the industry settles down.

Gius says Atmos Energy is handling most of its security in-house right now. "We pursued a number of open-source and lower-cost solutions to manage it ourselves," he says. "We invested in two people to help ensure we had the skills to manage that environment." But he'd like to outsource more if it makes sense financially. He notes that security is increasingly integrated into the platforms provided by the likes of Microsoft, Cisco and Oracle, as well as telecom providers like Comcast and Verizon. It makes sense to him to have those providers manage the security of their systems.

Beard, with SAIC, says that no matter what drives security spending decisions, companies should understand their specific security strategies and where managed security providers can offer unique value. Smart business executives understand that they must maintain control of the big picture at all times, even if a third party is managing many of the levers. Keeping an eye on security service providers and the risks they are encountering is essential. "CIOs and security officers may outsource certain functions to various degrees, but they should never outsource their responsibility," Beard advises.

Trend # 4

A New Corporate Commitment

CIOs may still struggle with the quality of their data security, but the response to this year's survey suggests their executive peers have agreed, finally, that security can't be ignored.

Companies' budget plans tell part of the story. Not only are more companies investing in security technologies, but overall security investments are largely intact, despite the economy.

Twelve percent of respondents expect their security spending to decline in the next 12 months. But 63 percent say their budgets will hold steady or increase (although fewer foresee increases than did last year).

For starters, more companies are hiring CSOs or chief information security officers (CISOs). Eighty-five percent of respondents said their companies now have a security executive, up from 56 percent last year and 43 percent in 2006. Just under one-third of security chiefs report to CIOs, 35 percent to CEOs and 28 percent to boards of directors.

Two factors are influencing companies to maintain security as a corporate priority: Seventy-six percent say the increased risk environment has elevated the importance of cybersecurity among the top brass, while 77 percent said the increasingly tangled web of regulations and industry standards has added to the sense of urgency.

Respondents were asked how important various security strategies had become in the context of harsher economic realities. Seventy percent cited the growing importance of data protection while 68 percent cited the need to strengthen the company's governance, risk and compliance programs.

Notes Mauricio Angée, senior manager of IT security and compliance and CSO at Universal Orlando: "For segregation of duty purposes, it's interesting to see how companies are being asked--by compliance auditors, qualified security assessors and through legislation--to hire IT security managers with a much-more-defined set of roles and responsibilities." Such roles include setting the company's security policy, making the security budget pitch (instead of the CIO) and delegating responsibility among lower-level IT security administrators and engineers.

How Cybercrime Costs You

Losses from incidents average $833,000.

The Business Impact of Security Breaches

- Financial Loss: 42%
- Brand or Reputation Compromised: 30%
- Intellectual Property Theft: 29%
- Home Page Altered or Defaced: 20%
- Fraud: 17%

(Multiple Responses Allowed)

None of these developments, however, make a focus on information security a sure bet in the eyes of IT leaders. Just because companies feel they have to spend money on security doesn't mean executives view it as an essential, even beneficial business process instead of a pain-in-the-neck task being forced upon them.

Angée said CIOs and security leaders still have to fight hard for every penny. Meanwhile, security execs don't have the same decision-making power as other C-level leaders in every company, says PricewaterhouseCoopers' Lobel. CIOs can bring in a CSO or CISO without a strategy and budget for that person to work with and end up achieving nothing. If something goes wrong, he concludes, "all you'll have is somebody to blame and fire."

Courtesy : Bill Brenner, CIO Magazine; www.computerworld.com
October 15, 2009

RESEARCH

The Top Five E-mail Mistakes to Avoid

A lousy e-mail system isn't just inconvenient, it will cost you business. It is not enough to spend money on a great-looking Web site and achieving a good rank on search engines if your e-mail system works against you. Just as your Web site carries the banner for your business, so too does your e-mail service. A shoddy system will cost you customers, and you probably won't even know that it's happening.

In this article I'll show you five typical e-mail mistakes that businesses make that are guaranteed to lose you business. And, in case you're making any of them now, I'll show you how to fix the problem.

Free E-mail Providers

Not only do free e-mail providers suggest that you're operating on the cheap by not paying for a "proper" e-mail service, but they're also a poor choice for your business. I'm not just talking about Hotmail and Gmail, but also about the e-mail service that you get when you sign up for an ISP service for your business.

If you're using an e-mail address that's linked to your internet service provider and you change providers, then you will lose your e-mail address. You would have to tell all your customers that your e-mail address has changed, which is not only a waste of time but the likelihood of you remembering everyone who needs your new address is slim; and you'll lose contact with those customers.

Worse still, by using a free e-mail provider, you miss out on a valuable way to advertise your business. My e-mail address, helen@helenbradley.com tells you that I have a Web site (www.helenbradley.com), and you can immediately go and learn more about me or my business. If I used an @hotmail.com address, you couldn't find my Web site from simply having my e-mail address, and my e-mail address wouldn't be contributing anything toward publicizing my business.

The simple solution, if your business has a domain name, is to have e-mail addresses which are someone @yourdomainname,com. With a little tinkering you can even set up your system to make use of the services provided by companies such as Gmail while still using @yourdomainname addresses. Then your customers simply e-mail and get replies from you using your domain-name linked e-mail address, and they don't need to know anything of how you manage these behind the scenes.

If you change ISPs or move to another hosting service, nobody needs to know. You don’t need to tell anybody and everything works as transparently as if the change didn't even happen.

Names in E-mail Addresses

This problem is a subtle one, but it is a big issue. If you create e-mail addresses that are in the form janesmith@yourdomainname.com, then you need to consider what happens should Jane leave your business. Any e-mails that Jane receives after she leaves your business have to be handled properly or you will lose customers.

Instead of having personalized e-mail addresses it is better to use specialties. For example, if Jane is a sales person, use sales@yourdomainname.com. Not only does your business look more professional but this flexible solution lets anyone handle Jane's email because they’re addressed to the sales department.

As long as you reply to your e-mails in a timely manner, your customers won’t notice the difference between sales@ or jane@ e-mail addresses. Also, you can still use individual signatures for these emails to personalize the replies. Good service is less about personal e-mail addresses than it is about actually answering e-mails quickly and professionally.

Redirecting E-mail

When someone is on vacation or away for more than a day, it’s vital that you redirect their e-mail to someone who can deal with them in their absence. This applies to jane@ type e-mail addresses or sales@ type ones. It’s almost impossible to redirect if someone uses personal e-mail addresses for business use which, as you'll see shortly, is a big NO.

At the very least, you need to send an out-of-office e-mail to the sender indicating that the person is away, telling them when the person will return and giving details as to what the sender should do in the meantime. Ideally though, the e-mail will just be redirected to someone who can reply to it.

E-mail is as important to an e-tailer as the phone is to a bricks-and-mortar business. The phone still gets answered when a receptionist is on vacation — don’t let e-mail sit unanswered just because someone is on vacation.

You should also ensure that out-of-office replies are removed immediately when the person returns from vacation. Customers won't be impressed if they e-mail and receive a reply saying the recipient will return on a date that has already passed.

Managing Former Employees

If someone a jane@ type e-mail leaves your business, do not cancel their account. Instead keep the account, change the account password and redirect incoming e-mail messages to someone else who can manage them.

If you cancel the account, the e-mail sent to that account will bounce back to the sender. You probably won't even know this is happening, and you won't know what business you are losing. Bouncing incoming e-mail due to canceled accounts tells your customers that you really don't care about their business.

On the other hand, if you redirect the e-mail to someone who can handle the replies and explain that the person has left the business, you have a chance at maintaining a good relationship with your customers.

Of course, you've probably already deduced that if your emails are the sales@ type addresses then this won't be an issue for you.

Mixing Business and Personal

One major mistake that people make is receiving personal and business e-mail at one e-mail address — it’s even worse if it’s a private e-mail address.

If you ever sell your business, you will need to decide whether the e-mail address goes with the business or not. A purchaser will see the contacts you have and the e-mail you receive as an integral part of your business and will want the address. You may not want to relinquish it if it give them access to all your personal e-mail as well.

If your employees get business e-mail sent to a personal address such as a Gmail or Hotmail address, then it will be impossible for you to get access to that e-mail if they leave. For this reason, don’t let anyone conduct business using accounts that you don’t control.

Courtesy : Helen Bradley; www.ecommerce-guide.com
November 3, 2009

OPINION

Lifestyle Hackers

why twenty-somethings skateboard right past security controls, and what it means for employers

The insider threat, the bane of computer security and a topic of worried conversation among CSOs, is undergoing significant change. Over the years, the majority of insider threats have carried out attacks in order to line their pockets, punish their colleagues, spy for the enemy or wreak havoc from within. Today's insider threats may have something much less insidious in mind—multitasking and social networking to get their jobs done.

There's a growing risk within most organizations today that is clearly an insider threat but is also clearly not caused by a disgruntled or disillusioned employee. In fact, the new insider threat is more likely to manifest itself as a gung-ho new employee or contractor. And more often than not, the new insider threat is a recently hired twenty-something. We've coined the term "lifestyle hacker" to refer to this new cadre of insider threats. The lifestyle hacker does not have malicious intent. Nevertheless, the lifestyle hacker is highly successful at skirting various corporate controls put in place to protect security-related websites and critical endpoints. The most interesting and ironic aspect of the lifestyle hacker is that he is motivated by the pursuit of productivity, often the very same motivation driving the implementation of various corporate controls (including but not limited to Web proxies, DLP solutions, firewalls, etc.).

Tightly managed organizations (especially huge financial corporations) often block access to Web 2.0 capabilities in order to "promote productivity of staff." However, this very same staff often desires to utilize Web 2.0 capabilities (including social networking, external IM, Skype, Twitter, etc.) in the name of enhancing personal productivity. And never the twain shall meet!

This conundrum exists as the inherent conflict between those who make the rules and those who break the rules, both of whom are driven by the exact same motivation—being more productive in the work environment. There are two fascinating and problematic aspects of this situation worth mentioning:

1. The population of lifestyle hackers is growing in size and diversity as demographics of new hires shift toward those people who grew up on the Internet.

2. Neither the corporate decision makers who make the rules nor the lifestyle hackers understand the security ramifications of emerging and evolving Web 2.0 capabilities (see McGraw's article "Twitter Security" at www.informit.com/articles/article.aspx?p=1350268).

To get a handle on the growth of the lifestyle hacking problem, consider this: One Wall Street firm we're both very familiar with estimated that 45 percent of all security incidents in the past two years were lifestyle hacks. A quick look at demographics reveals what's going on. The root of the problem is that newly minted staff members being hired today were generally born in the late '80s; their managers and rule-imposers are of the Baby Boom generation (born between 1947 and 1961). Baby Boomers were brought up with television as the dominant household technology, while the Net Generation (as Don Tapscott calls them in Growing Up Digital: The Rise of the Net Generation) was exposed to the Internet as early as they can remember (and some even earlier than that). Television is a mostly passive broadcast medium. By contrast, the Internet promotes widespread collaboration. This difference engenders significant divergence in behavior for the two generations. Baby Boomers focus on a single task when under pressure, while the Net Generation prefers multitasking.

Baby Boomers don't even like listening to music while they work. Net Gen'ers listen to music (sometimes even watching music videos) while browsing a website or six, instant-messaging with whoever is around, sending text messages and pecking at a Microsoft Office file. The University of Oregon Library published a study that showed that the average Net Gen'er, by the age of 21, has been exposed to:

- ❖ 10,000 hours of video games
- ❖ 200,000 e-mails
- ❖ 20,000 hours of TV
- ❖ 10,000 hours of cell phone conversation
- ❖ Less than 5,000 hours reading books

Some demographers bifurcate the Net Generation into Generation X and Y, but for the purposes of understanding the lifestyle hacker, Net Gen says it all. As Internet-facing technology became ubiquitous and leaped from the home to the mobile device, the Net Generation adapted by incorporating new technology into its very social fabric. The Net Generation prefers SMS texting and using instant messaging in many social situations. (Organizing a particular time and place to meet is rather silly if the people doing the meeting all have cell phones and a vague plan.)

Utilizing a texting system as an essential productivity tool in a professional environment is a natural extension of normal Net Gen social behavior. The same can be said for social networks such as Facebook, which offer excellent tools for collaborating on complex problem solving and building effective relationships.

Unfortunately, many Baby Boomers have never used Web 2.0 tools at work. Such tools simply did not exist when they entered the work force. As a result, they often view such tools as distractions from doing "real" work.

One high-tech firm did a study on the primary reason for undergraduate offer rejections by prospective new hires and discovered that the number-one reason for rejection was that access to Facebook was blocked. The firm now offers access to Facebook. Along the same lines, but without a solution to the problem, FS-ISAC survey results from April 2009 indicated that over 90 percent of financial service firms block access to social networking sites. The number-one reason for blocking access is a concern over productivity, not security. Ninety-five percent of the firms responding to the survey have no plans to change policies to allow access to social networking sites. You can see the storm clouds gathering.

To restate the conundrum, leaders believe that social networking, instant messaging and using SMS constantly in the work environment will lead to lower overall productivity, so they block access. Net Gen'ers believe that Web 2.0 technologies are essential for collaboration and relationship management and that they improve productivity. Impasse.

Enter the lifestyle hacker. To sidestep the impasse, a growing number of Net Gen'ers are using their technical savvy to find creative ways of bypassing controls so they can leverage Web 2.0 capabilities. Perhaps an example can make this clear.

Dylan (not his real name) was an intern working in the technology department doing server administration for two years while he completed graduate school. He then applied for and was hired as an analyst working in the operational risk department. Dylan established himself as an effective contributor to the department over a period of six months.

One day, the corporate security staff noticed a spike in network traffic coming from Dylan's workstation. The large volume of data transfer indicated the possibility of a security breach in which company information was being shoveled off to an outside party. The security staff initiated an investigation. They eventually approached Dylan and completed a forensic analysis of his computer. What they uncovered was that Dylan had constructed a secure tunnel by exploiting a vulnerability in the company's Web proxy, and he was connecting his workstation to his ISP at home. This allowed Dylan to watch pirated movies running on his home PC while he was streaming music from sites no longer filtered by the proxy.

As it turns out, Dylan was also modifying a sensitive risk report at the same time. When Dylan's boss was told what was going on, Dylan was asked to leave the firm. His boss was disappointed, since Dylan was one of her most productive employees.

Note that Dylan was not malicious and in fact did not intend to break established policies and federal laws. His actions were motivated purely by his desire to multitask, unfettered by the standard controls that all other employees had to live with.

The question is, how many "Dylans" work in your organization? And what are you to do if you're the CSO trying to safeguard your firm while also enabling business growth? As usual for computer security, there are no easy answers here, just as there are no simple Web 2.0 technology controls ready for prime-time implementation.

Upon reflection, we believe the most important thing to do is to educate staff about the security and brand risks associated with unfettered use of Web 2.0 capabilities while exploring ways to offer tools with collaborative capabilities with a level of control that the organization can manage effectively.

This solution is likely to necessitate updating your security policies as well as communications and marketing policies governing publication of the firm's information. In addition, the firm's IT strategy should clearly define a road map for Web 2.0 implementation over time that provides for increased collaboration outside the firm. The right approach for each organization must, of course, be driven by its respective business model, since business and security risks always differ. The good news is that the problem of the lifestyle hacker provides a clear opportunity for innovative leadership by the CIO and the CSO.

What is clear is that the technology frontier has moved well beyond the workstation to an increasing constellation of mobile devices and distributed software (some of it already in the cloud). As more processing capability emerges in PDAs, there will be no avoiding them or their distributed software as a work platform. Collaborative technology is here to stay.

Solving the Net Gen productivity problem in order to avoid lifestyle hacking is thus a critical aspect of the CSO's job. Finding the right balance for your organization will require innovation, education and, most importantly, courage. We certainly can't hold back Web 2.0 in the name of security! At least not for long.

Courtesy : Jim Routh and Gary McGraw; CSO; www.csoonline.com
November 02, 2009

COMMENTS

Malware Makers Are Organized, Sophisticated

Cybercriminals are organized like corporations, and follow regular software release cycles

Malware makers – the criminals responsible for viruses and worms – have become increasingly organized and sophisticated, according to a Microsoft security report that was released today. Gamers, the gullible, USB drive users, and people who don't patch their PCs are their biggest targets.

Cybercriminals are organized like corporations, and follow regular software release cycles, said Jeff Williams, principal group program manager for the Microsoft Malware Protection Center: "They are working for monetary gain."

The report, entitled, Microsoft Security Intelligence Report Volume 7, is based upon data collected worldwide from January through June 2009. The data was obtained through Microsoft's security products, Hotmail, and Windows Update, Williams said. "It shows differences from region to region, and provides a comprehensive view of the threat landscape."

Globally, Microsoft found that the number of trojan downloaders has fallen markedly over the past year; although, they did remain the most common threat. That gain was offset by a rise in instances of worms, password stealers and monitoring tools, according to the report.

Malware has been increasingly targeting online gamers, and there has been a major uptake in fraudulent security software, Williams said. Criminals create trojan software that purports to protect users from malware, but does nothing more than steal personal information and obtain credit card information through false premise.

Criminals have also begun the practice of bundling malware, and making "pay for play" arrangements with one another, Williams said. Another trend Williams noted is the misuse of autoplay in Windows, and using removable media like USB jump drives as an attack vector to get inside of protected enterprise environments.

Microsoft recommends that customers should use trusted anti virus software, a Web browser with anti-phishing technology, and keep their operating systems up-to-date. Security software, combined with increased industry and government cooperation, has helped Microsoft better protect customers over the past year, Williams said.

However, Microsoft is playing a game of multidimensional chess against an opponent that is profit-driven. Improvements in security have induced cyber criminals to exploit more complex software vulnerabilities, and those vulnerabilities have become the new chosen mechanisms for propagating worms of worms, Williams acknowledged.

“They left a note in a worm telling us that they would take more direct action in the future. Criminals are becoming more aggressive,” Williams said. Simply put, when one door closes, they find another.

With Windows becoming more secure, third party applications are being targeted with rising frequency, Williams noted. To combat that threat, Microsoft has delivered free security tools to developers, along with documentation on the steps that it takes internally to create secure software.

Thankfully, other major software companies including HP and IBM have bought security firms, and are making efforts to secure their software. A lot of the industry still lags, but steady progress is being made.

A security expert once told me that hackers were the highwaymen of our century. Highwaymen were thieves that preyed upon travelers during the Elizabethan era. They became obsolete when society created toll roads–closing off their route of escape–and increased police patrols. The crime was not worth the time.

Software is exceedingly more complex than road building, and modern operating systems are some of the most advanced things man has ever created. It’s not really possible to make software that is entirely secure. Even still, I have confidence that enough progress will be made to raise the risks and reduce the gains of cybercrime.

Courtesy : David Worthington, Technologizer; www.pcworld.com
Nov 4, 2009

SURVEY

IT Workers Building Security Into Their Career Strategies

More tech professionals seeking security certifications

IT professionals are placing their bets on security as they plot their next career moves, according to a new study published earlier today.

The survey of more than 1,500 IT workers, which was conducted by the IT trade association CompTIA, found that 37 percent intend to pursue a security certification over the next five years. Another 18 percent of IT workers said they will seek ethical hacking certifications during the same time period, while 13 percent identified forensics as their next certification target.

"Given the growing reach of security, with threats becoming more pervasive and dangerous and with no business or industry immune to those threats, it makes sense that many IT professionals view this as a must-have for career advancement," said Terry Erdle, senior vice president, skills certifications for CompTIA.

Other technology areas where survey respondents said they will seek new certifications over the next five years include green IT, healthcare IT, mobile and software-as-a-service.

Economic advancement and personal growth are key drivers for seeking IT certifications, the CompTIA study also reveals. Eighty-eight percent of certification holders indicated they pursue a certification to enhance their resumes. An identical 88 percent said personal growth is a major or minor reason in their decision to pursue a certification.

IT workers are willing to invest the time and resources necessary to get the certifications, CompTIA says. On average, candidates for an IT certification spend 44.5 hours studying and preparing to sit for an exam; and approximately one in three individuals spend 60 or more hours preparing. Fifty percent of IT certification holders pay for the exams themselves, while 38 percent rely on an employer to cover the exam fee.

The web-based survey was completed by 1,537 IT professionals during the period from July 13 through July 31, 2009. Survey participants were primarily from the United States, Canada and the United Kingdom.

Courtesy : CompTIA study; Tim Wilson; www.darkreading.com
Nov 04, 2009

LAW

What is cyberterrorism? Even experts can't agree

(The Harvard Law Record Report)

Cyberterrorism is a buzzword that has been thriving in the administration of President Barack Obama, but it has such a nebulous meaning that it managed to elude three expert panelists last Wednesday.

Leonard Bailey was transferred from the Department of Justice's (DOJ) Computer Crimes and Intellectual Property Division to the administration's new National Security Division (NSD), in September 2009 to spearhead the team's cybercrime efforts.

According the NSD's press release, "Mr. Bailey is widely respected within the Justice Department and the Intelligence Community for his knowledge of cyber issues." However, even he admitted he is at a loss for words on the subject. The area suffers from a "limited lexicon," he explained, "we even lack a unified definition of cyberterrorism and that makes discourse on the subject difficult."

The government has failed to convene its various departments to forge a single definition. The FBI alone has published three distinct definitions of cyber-terrorism: "Terrorism that initiates…attack[s] on information" in 1999, to "the use of Cyber tools" in 2000 and "a criminal act perpetrated by the use of computers" in 2004. Other government agencies responsible for responding to cyberattacks, such as the Department of Defense, Federal Emergency Management Agency, National Infrastructure Protection Center, Drug Enforcement Agency, National Homeland Security Agency, and the Department of Justice have each created their own definitions.

Bailey's explanation for the limited and conflicting vocabulary is twofold. First, "the interest in cyber issues only started in the nineties so the terms are still nascent." Secondly, the departments have fragmented the definition because the meaning depends on their differing interests. "Look at the response to Twitter," he observed. "The Department of State lauded its use in Iran, while other departments heavily criticized it."

Unlike Bailey, Kim Taipale, founder and executive director for the Stilwell Center for Advanced Studies in Science and Technology Policy believes "cyberterrorism, whatever it is, is a useless term." Taipale believes that, "terrorists will use any strategic tool they can" so "cyber" terrorism is no more important then other forms. Rather the problem is that there is no "unified legal regime," creating a "gap between law-makers and authorities," he stated. "Whether the military or police should respond, whether it is domestic or foreign is not fully determined," said Taipale. These separate entities are "incompatible and inconsistent, making us more vulnerable to terrorism."

Taipale explained that having such a fragmented legal structure means that we are "not equipped to deal with an array of a whole host of new problems" that cyber issues present. And this is truly troublesome because the line between "safe society and chaos is a thin one," said Taipale, "We are in line for some serious cyber-Katrinas that we are not ready to deal with."

Like Bailey, however, Taipale believes that the "obsolete security infrastructure" exists because different entities have differing concerns. After cyber-threats were made to Slobodan Milosevic's bank accounts during the 1999 Kosovo crisis, for example, the cyberterrorism discussion was raised in the U.N., and although Russia expressed interest in the problem, the U.S. stalled the discussion. "What is and isn't permissible was never decided because of the U.S.' interest in its own international liability," said Taipale. "Now there are no rules," he continued. "Now we are reaping the problems."

Taipale's fear that the line between safe society and chaos is fragile is compounded by the problem of trust, highlighted by Dr. Andrew Colarik, an information security consultant. Colarik stressed the term's etymology, saying that "there is no cyberterrorism without terrorism." In essence, the goal of terrorism is to cause severe disruption through widespread fear in society, meaning "our dependency on digital material," is the problem, he said. "The majority of our currency is not paper, it's digital. And like money, if we loose confidence in the underlying system, we will have insolvency." Colarik argues that we should limit the amount of information we store digitally.

Taipale echoed the doomsday concern, "the U.S. is a real target because of our dependency on the online system." These attacks are about "exploitation." "Non-peer" countries don't depend on the digital system and so they have an opportunity to attack without the risk of suffering from similar counterattacks.

But Bailey believes the problems Taipale and Colarik raise cannot be solved without some basic agreement over terminology. "These are conversations that cannot take place because there is no common language to discuss this," he said. He suggests as a first step "that we as a government have to consider what we think about these issues first." The hesitation is that "whatever you decide you have to live with." While it is possible that trying to divine a definition of cyberterrorism is a fools' errand, "it is a way of achieving an end."

Courtesy : Victoria Baranetsky; www.hlrecord.org
November 6, 2009

REPORT

SMEs lack cybersecurity awareness and policies

Small and Medium Enterprises (SME) are slowly but surely embracing technology, they are incorporating it to their business operation. They want to become more efficient, more effective and more organized. SMEs operate in a simple and straightforward fashion, they may use technology but you will seldom find a SME with its own I.T. department.

The I.T. department of most SMEs is the computer or laptop itself. For this reason, while technology is helping them in doing their businesses, some aspects of technology are being compromised - like security.

According to the 2009 National Small Business Cybersecurity Study shows small business owners' cybersecurity policies and actions are not adequate enough to ensure the safety of their employees, intellectual property and customer data. The study, co-sponsored by the National Cyber Security Alliance (NCSA) and Symantec surveyed nearly 1,500 small business owners across the United States about their cybersecurity awareness policies and practices.

The survey confirmed that small businesses today are handling valuable information - 65% store customer data, 43% store financial records, 33% store credit card information, and 20% have intellectual property and other sensitive corporate content online. 65% of the business survey claimed that the Internet was critical to their businesses success yet they are doing very little to ensure that their employees and systems are not victims of a data breach.

The study shows

- 86 percent do not have a staff dedicated to IT security
- 53 percent check their computers on a weekly basis to ensure that anti-virus, anti-spyware, firewalls and operating systems are updated; 11 percent said they never check at all
- 25 percent of the businesses do not ensure password protection for their wireless networks
- 66 percent of employees take computers or PDAs containing sensitive information off-site

- 72 percent do not have formal Internet security policies

Meanwhile, small businesses seem out of sync with some Internet security risks. 75% small businesses said that they use the Internet to communicate with customers yet only 6% fear the loss of customer data and only 42% believe that their customers are concerned about the IT security of their business. What's more, 56% of small businesses believe cybersecurity is the cost of doing business while 21% believe it is just "a nice thing to have."

Laptops, PDAs and wireless networks are great conveniences to businesses, yet they carry with them an added responsibility to ensure the data is secure. Today, more than 66% of employees take computers or PDAs containing sensitive information off-site. Wireless networks are gateways for hackers and cyber criminals and must be secured by complex passwords. Unsecured wireless networks are akin to leaving the front door of a filing cabinet wide open on the sidewalk. 62 percent of the companies surveyed have a wireless network but 25 percent of them do not password protect their wireless networks. This is a significant security risk as hackers can steal information being passed through these open networks.

Remember that security awareness and education, combined with a comprehensive security solution, can empower small businesses and their employees to protect themselves and their information. It is the responsibility of technology solutions providers or even hardware providers to inform SMEs about the possible threats - do not be just their technology providers, be their partners and you will have more business that you can imagine.

Courtesy : JERRY LIAO; www.mb.com.ph
November 4, 2009

INVESTIGATION

You Can be Framed for Child Porn by a PC Virus

Of all the sinister things that Internet viruses do, this might be the worst: They can make you an unsuspecting collector of child pornography.

Heinous pictures and videos can be deposited on computers by viruses — the malicious programs better known for swiping your credit card numbers. In this twist, it's your reputation that's stolen.

Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught. Pranksters or someone trying to frame you can tap viruses to make it appear that you surf illegal Web sites.

Whatever the motivation, you get child porn on your computer — and might not realize it until police knock at your door.

An Associated Press investigation found cases in which innocent people have been branded as pedophiles after their co-workers or loved ones stumbled upon child porn placed on a PC through a virus. It can cost victims hundreds of thousands of dollars to prove their innocence.

Their situations are complicated by the fact that actual pedophiles often blame viruses — a defense rightfully viewed with skepticism by law enforcement.

"It's an example of the old `dog ate my homework' excuse," says Phil Malone, director of the Cyberlaw Clinic at Harvard's Berkman Center for Internet & Society. "The problem is, sometimes the dog does eat your homework."

The AP's investigation included interviewing people who had been found with child porn on their computers. The AP reviewed court records and spoke to prosecutors, police and computer examiners.

One case involved Michael Fiola, a former investigator with the Massachusetts agency that oversees workers' compensation.

In 2007, Fiola's bosses became suspicious after the Internet bill for his state-issued laptop showed that he used 4 1/2 times more data than his colleagues. A technician found child porn in the PC folder that stores images viewed online.

Fiola was fired and charged with possession of child pornography, which carries up to five years in prison. He endured death threats, his car tires were slashed and he was shunned by friends.

Fiola and his wife fought the case, spending $250,000 on legal fees. They liquidated their savings, took a second mortgage and sold their car.

An inspection for his defense revealed the laptop was severely infected. It was programmed to visit as many as 40 child porn sites per minute — an inhuman feat. While Fiola and his wife were out to dinner one night, someone logged on to the computer and porn flowed in for an hour and a half.

Prosecutors performed another test and confirmed the defense findings. The charge was dropped — 11 months after it was filed.

The Fiolas say they have health problems from the stress of the case. They say they've talked to dozens of lawyers but can't get one to sue the state, because of a cap on the amount they can recover.

"It ruined my life, my wife's life and my family's life," he says.

The Massachusetts attorney general's office, which charged Fiola, declined interview requests.

At any moment, about 20 million of the estimated 1 billion Internet-connected PCs worldwide are infected with viruses that could give hackers full control, according to security software maker F-Secure Corp. Computers often get infected when people open e-mail attachments from unknown sources or visit a malicious Web page.

Pedophiles can tap viruses in several ways. The simplest is to force someone else's computer to surf child porn sites, collecting images along the way. Or a computer can be made into a warehouse for pictures and videos that can be viewed remotely when the PC is online.

"They're kind of like locusts that descend on a cornfield: They eat up everything in sight and they move on to the next cornfield," says Eric Goldman, academic director of the High Tech Law Institute at Santa Clara University. Goldman has represented Web companies that discovered child pornographers were abusing their legitimate services.

But pedophiles need not be involved: Child porn can land on a computer in a sick prank or an attempt to frame the PC's owner.

In the first publicly known cases of individuals being victimized, two men in the United Kingdom were cleared in 2003 after viruses were shown to have been responsible for the child porn on their PCs.

In one case, an infected e-mail or pop-up ad poisoned a defense contractor's PC and downloaded the offensive pictures.

In the other, a virus changed the home page on a man's Web browser to display child porn, a discovery made by his 7-year-old daughter. The man spent more than a week in jail and three months in a halfway house, and lost custody of his daughter.

Chris Watts, a computer examiner in Britain, says he helped clear a hotel manager whose co-workers found child porn on the PC they shared with him.

Watts found that while surfing the Internet for ways to play computer games without paying for them, the manager had visited a site for pirated software. It redirected visitors to child porn sites if they were inactive for a certain period.

In all these cases, the central evidence wasn't in dispute: Pornography was on a computer. But proving how it got there was difficult.

Tami Loehrs, who inspected Fiola's computer, recalls a case in Arizona in which a computer was so "extensively infected" that it would be "virtually impossible" to prove what an indictment alleged: that a 16-year-old who used the PC had uploaded child pornography to a Yahoo group.

Prosecutors dropped the charge and let the boy plead guilty to a separate crime that kept him out of jail, though they say they did it only because of his age and lack of a criminal record.

Many prosecutors say blaming a computer virus for child porn is a new version of an old ploy.

"We call it the SODDI defense: Some Other Dude Did It," says James Anderson, a federal prosecutor in Wyoming.

However, forensic examiners say it would be hard for a pedophile to get away with his crime by using a bogus virus defense.

"I personally would feel more comfortable investing my retirement in the lottery before trying to defend myself with that," says forensics specialist Jeff Fischbach.

Even careful child porn collectors tend to leave incriminating e-mails, DVDs or other clues. Virus defenses are no match for such evidence, says Damon King, trial attorney for the U.S. Justice Department's Child Exploitation and Obscenity Section.

But while the virus defense does not appear to be letting real pedophiles out of trouble, there have been cases in which forensic examiners insist that legitimate claims did not get completely aired.

Loehrs points to Ned Solon of Casper, Wyo., who is serving six years for child porn found in a folder used by a file-sharing program on his computer.

Solon admits he used the program to download video games and adult porn — but not child porn. So what could explain that material?

Loehrs testified that Solon's antivirus software wasn't working properly and appeared to have shut off for long stretches, a sign of an infection. She found no evidence the five child porn videos on Solon's computer had been viewed or downloaded fully. The porn was in a folder the file-sharing program labeled as "incomplete" because the downloads were canceled or generated an error.

This defense was curtailed, however, when Loehrs ended her investigation in a dispute with the judge over her fees. Computer exams can cost tens of thousands of dollars. Defendants can ask the courts to pay, but sometimes judges balk at the price. Although Loehrs stopped working for Solon, she argues he is innocent.

"I don't think it was him, I really don't," Loehrs says. "There was too much evidence that it wasn't him."

The prosecution's forensics expert, Randy Huff, maintains that Solon's antivirus software was working properly. And he says he ran other antivirus programs on the computer and didn't find an infection — although security experts say antivirus scans frequently miss things.

"He actually had a very clean computer compared to some of the other cases I do," Huff says.

The jury took two hours to convict Solon.

"Everybody feels they're innocent in prison. Nobody believes me because that's what everybody says," says Solon, whose case is being appealed. "All I know is I did not do it. I never put the stuff on there. I never saw the stuff on there. I can only hope that someday the truth will come out."

But can it? It can be impossible to tell with certainty how a file got onto a PC.

"Computers are not to be trusted," says Jeremiah Grossman, founder of WhiteHat Security Inc. He describes it as "painfully simple" to get a computer to download something the owner doesn't want — whether it's a program that displays ads or one that stores illegal pictures.

It's possible, Grossman says, that more illicit material is waiting to be discovered.

"Just because it's there doesn't mean the person intended for it to be there — whatever it is, child porn included."

Courtesy : JORDAN ROBERTSON; AP Technology Writer
Nov 9, 2009