M86 SECURITY

Strengthening Your Defenses: Web Security and Inbound Malware Protection

Education Thought Leadership Series

The interactive Internet and emerging Web 2.0 resources are changing how educators teach, students learn, and administrators lead. Likewise, sophisticated networks and enterprise applications are being employed to manage the administrative functions of educational organizations. These networks of applications, information, resources, and capabilities for instant communications enable school leadership to manage more efficiently and make decisions more effectively. Throughout this evolution and exploration of these online environments, the importance of cyber-security cannot be ignored. It is the responsibility of school district leadership to understand emerging security issues, embrace their roles as leaders, and assume responsibility for the proper protection of student information, financial data, and the management of school district resources in this constantly evolving and changing digital world.

School districts and educational institutions are not immune to the network security breaches that have faced retail, banking, and government organizations across our nation and around the world. This white paper articulates the risks associated with assuming the "it will not happen to us" position, reviews the deficits of a number of current malware and web protection strategies, and outlines approaches designed to meet the emerging security needs of education in a manner that is both comprehensive and cost effective.

K-12 SECURITY BREACHES

In November [2009], the federal Internet Crime Complaint Center (IC3) had issued an "intelligence note," reporting that the FBI had seen a significant increase in fraud involving "the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts."[1] This section of the white paper presents examples of K-12 security breaches with significant negative impact on K-12 school systems. Three of these cases involved the theft of district funds through unauthorized online transfers. Three of the cases presented experienced loss of time, productivity, and critical network access during the cyber attack and recovery period.

The three school districts experiencing attacks on their banking accounts include:

- Crystal Lake School District, Illinois, June/July 2009[2]
- Western Beaver County School District, Pennsylvania, July 2009[3]
- Duanesburg Central School District, New York, December 2009[4]

In late June and early July of 2009, the **Crystal Lake School District** lost more than $325,000 when a virus infected school district computers, stole banking credentials, and siphoned off funds from the district's bank accounts. Periodic monitoring of the district bank accounts noted irregularities that immediately prompted further investigation leading to the eventual discovery of the unauthorized transactions. "Though it's impossible for a school district to be completely immune to cyber attacks, [Superintendent] Mendoza said district officials should take steps to minimize opportunities for cyber criminals to compromise their networks."[5]

Western Beaver County School District is one of a number of school districts where the FBI is currently investigating online computer intrusions that have resulted in thousands of taxpayer dollars being stolen. In July of 2009, malicious software was used to transfer more than $700,000 in 74 separate transactions over a two-day period from this western Pennsylvania school district before being noticed.

Duanesburg Central School District learned of fraudulent activity when their bank questioned the validity of a request for an electronic transfer of funds to multiple overseas accounts on December 22, 2009. Upon confirming that the pending requests totaling approximately $759,000 were not legitimate, they were immediately cancelled. This discovery began an in-depth investigation that revealed an additional $3 million in unauthorized electronic transfers had already been executed during the previous two days. As of early 2010, the school district has recovered $2.5 million of the stolen funds, leaving nearly $500,000 still missing.

The Trojan.Clampi is suspected as the virus used in the above breaches that enabled thieves to harvest the victim's business or corporate bank account login information. The virus is planted on unwitting users' computers by sending out what appears to be an e-mail message from a trusted source that actually includes a malware link or an infected attachment. Once the user clicks the link or opens the attached file, the banking Trojan is planted on his or her computer.[6] "It's well known that malware is growing more sophisticated, but few threats have had us scratching our heads like the Trojan. Clampi," a researcher Patrick Fitzgerald from Symantec Corp. wrote. "Trojan.Clampi has been around for a number of years now. During this time it has gone through many iterations, changing its code with a view to avoid detection and also to make it difficult for researchers to analyze."[7]

"The Federal Crimes Enforcement Network, a Treasury Department division that tracks suspected cases of fraud reported by banks said incidences of wire-transfer fraud rose 58% in 2008. But experts say reliable figures about losses from commercial online banking fraud are hard to come by, and many incidents go unreported."[8]

The three school districts experiencing broad scale, network disabling cyber attacks include:

- Vancouver School District, Canada, January 2009[9]
- Chariho School District, Rhode Island, May 2009[10]
- Eugene School District, Oregon, January 2010[11]

A non-destructive, but constantly replicating virus struck the **Vancouver, Canada** school district in early January of 2009. No district data was compromised and no personal information was placed at risk, but it took nearly a week to contain the virus and cleanse the system. District leadership noted that updated anti-virus was installed at the time of the incursion but did not identify the invading program because it had not yet been identified as a virus.

Chariho School District computers were infected and then re-infected by the Qbot virus in May 2009 disabling the school district's approximately 1,100 computers and website for over a week. This insidious virus steals information while users type, remembering each keystroke for future malicious attacks. The entry point of the virus into the district network may never be determined. The Qbot virus did not breach the district's data systems that store personnel information. District leadership estimates that the repair and recovery from their attack will cost the district upwards of $25,000.

In January of 2010, district IT staff at the **Eugene School District** noticed unusual activity on a department server. Upon investigation, they discovered that hackers had breached the security of a server containing contact information of current and former Eugene School District employees. The server in question did not include other personal information but was attached to servers that did contain Social Security numbers and other sensitive data. It is unknown if this information was stolen, but is considered a possibility, thus, this breach may have involved information for 26,000 individuals and district vendors. To some degree, the uncertainty is as damaging as the reality.

Each of these specific examples presents both the diversity and destructiveness of known and unknown malware impacting school districts with greater and greater frequency. The following statistics demonstrate the breadth and growth of these emerging challenges:

- According to M86 Security Labs, even with adequate protection from Antivirus software, Zero Day Vulnerabilities left users vulnerable to potential attacks 40% of the time in the 2nd half of 2009.[12]
- In their July 2009 update, Sophos reports 23,500 new infected web pages are discovered every day, the US hosts more malware and relays more spam than any other country, and 22.5 million different samples of malware exist in the collection of independent testing agency, AV-Test.org.[13]
- The Google Security Team noted in August of 2009 that the number of entries on their malware list has more than doubled in one year and they have seen periods in which 40,000 web sites were compromised per week.[14]
- The Kaspersky bulletin states that 2009 was the latest milestone both in the history of malware and in the history of cybercrime, with a marked change in direction in both areas . . . with the number of malicious programs in the Kaspersky Lab collection reaching 33.9 million.[15]
- Websense® Security Labs™ identified a 233% growth in the number of malicious sites during the first half of 2009 and 671% growth in the number of malicious sites during the last year.

From the Sophos report, "Today, most organizations have guarded their email gateways and broadened their defenses against email-borne malware and malicious spam. Consequently, cybercriminals are developing techniques to infect machines behind-the-scenes by embedding malicious code on innocent websites and luring victims to them."[13]

These stories and statistics highlight the potential negative consequences of a variety of online security breaches. Next, this white paper outlines Security Protection Considerations for districts deciding to take a proactive stance versus the traditional reactive approach seen in the examples presented.

From the Kaspersky report, "A standard antivirus solution of the 1990s (scanner and monitor) still offered the requisite level of protection in 2006. However, by 2009 this protection was no longer grounded in reality, and had effectively been replaced by combination solutions – Internet Security products which integrated a wide range of technologies to offer defense in depth."[15]

SECURITY PROTECTION CONSIDERATIONS

Today, the threat landscape for network security is complex and constantly evolving. Web 2.0 has created increased demand for bandwidth to deliver the digital content our schools need. In this effort, the importance of delivering safe and secure digital content is critical. Learning organizations must continuously assess and enhance as needed the security protection measures as part of their network and information security plan. Attempting to keep pace with the evolving threats aligned with the complexity of the systems and the devices being supported can be an overwhelming task. What must IT leaders consider to protect information, networks, and most importantly students, teachers, and staff from the security risks of a Web 2.0 enabled world?

All organizations today need network and information security. To achieve acceptable levels of security, each organization must define what needs to be protected

and why. What security protection measures, if any, are district technology leaders willing to leave unaddressed or ignored? What are the risks and benefits of making these decisions? The challenge facing IT leaders is to provide for the safety and security of information, students, teachers, and staff within budgetary constraints. The following table, although not comprehensive or prioritized, attempts to address the "what are we protecting and why" question.

What are we protecting?	Why?
Network and Computing Assets/Resources	In order to support the core mission of the school, it is necessary to protect and provide a consistent and reliable digital infrastructure.
Learning and Productivity	This is the core mission of our educational organizations. How do you measure lost learning opportunities if resources are unavailable or negatively impacted? How much productivity is lost in the organization responding to a network security issue?
Reputation and Perception	The loss of any organization's reputation due to network security and the resulting negative communications can have a substantial and quite serious long-term impact, including significant financial impact.
Financial Loss	Schools, like all businesses, need to protect the financial assets of the organization. Most school's financial assets have moved to online banking, exposing these resources to increased risk. A significant number of schools have been victims of Phishing attacks providing hackers access to the school's financial accounts.
Access Credentials	Loss of accounts and passwords to systems and network resources could be devastating if in the wrong hands. What would happen if the administrator password to your student information system became compromised without your knowledge?
Performance and Service Availability	Denial of service or performance results in loss of maximum performance from the network and computing services and resources. These vulnerabilities can come in many ways and often create frustration and are extremely disruptive to the day-to-day objectives of the organization.
Protected Information and Identity Theft	With a few matching data elements, a person's life can be severely and negatively impacted. It is the responsibility of all learning organizations to address this area. Also, a digital information or identity theft security plan is required in many states to assure the security of information that is protected by various laws such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Gramm Leach Bliley Act (GLBA), and others. States with regulations include California, New Jersey, Rhode Island, Massachusetts, and Nevada.
People (Students, Teachers, Staff)	The ultimate and overarching goal is protecting people from harmful, threatening, and ill-intentioned network predators, malicious software (malware) and the long-term impact these threats will have on their lives.
Quality of User Experience	The user experience is important, and when the network and computing is not providing the quality expected or designed, the impact is felt throughout the organization.
Increasingly Mobile User	The user and their devices are now moving from place to place inside and outside the network. How are the security controls in place on your internal network going to cover these remote users? What impact does this have on your information and network security?
Access to Harmful Content	The Children's Internet Protection Act requires that all schools receiving E-rate funds have in place a content filtering solution to protect children from harmful digital content.

A combination of people, processes, and technology are required to ensure that each of these factors, and those not listed, are addressed and protected. In addition, there are linkages between each that create a cascade effect, where one area may impact another area and at potentially different levels. For example, a denial of service attack can happen on a single computer (a network asset), which potentially may impact the information technology department's reputation within the organization. The consequences of an attack depends on other factors as well, such as the victim, the impact the attack had on the ability of the organization to meet its goals and objectives, and the timing of the breach. The impact of a security breach can be viewed as a "house of cards" if and when the organization becomes a victim.

The following model presents a visual framework in the development of a comprehensive plan to address the network and information security challenges for a learning organization. This multi-layered approach is designed to address the people, process and solutions necessary. Two important first steps required of the organization include:

- Create a role/position for Network and Information Security Officer (NISO)
- Draft, approve, and implement the organization's Network and Information Security Plan (NISP)

Create a Role/Position for Network and Information Security Officer (NISO)

A Network and Information Security Officer should be assigned responsibility to lead the development of the Network and Information Security Plan. In addition, the NISO should have the authority to issue authorization to operate an information system under specific guidelines as well as the authority to deny operation of any information system or service. The NISO is responsible for all issues regarding the network and information security for the organization.

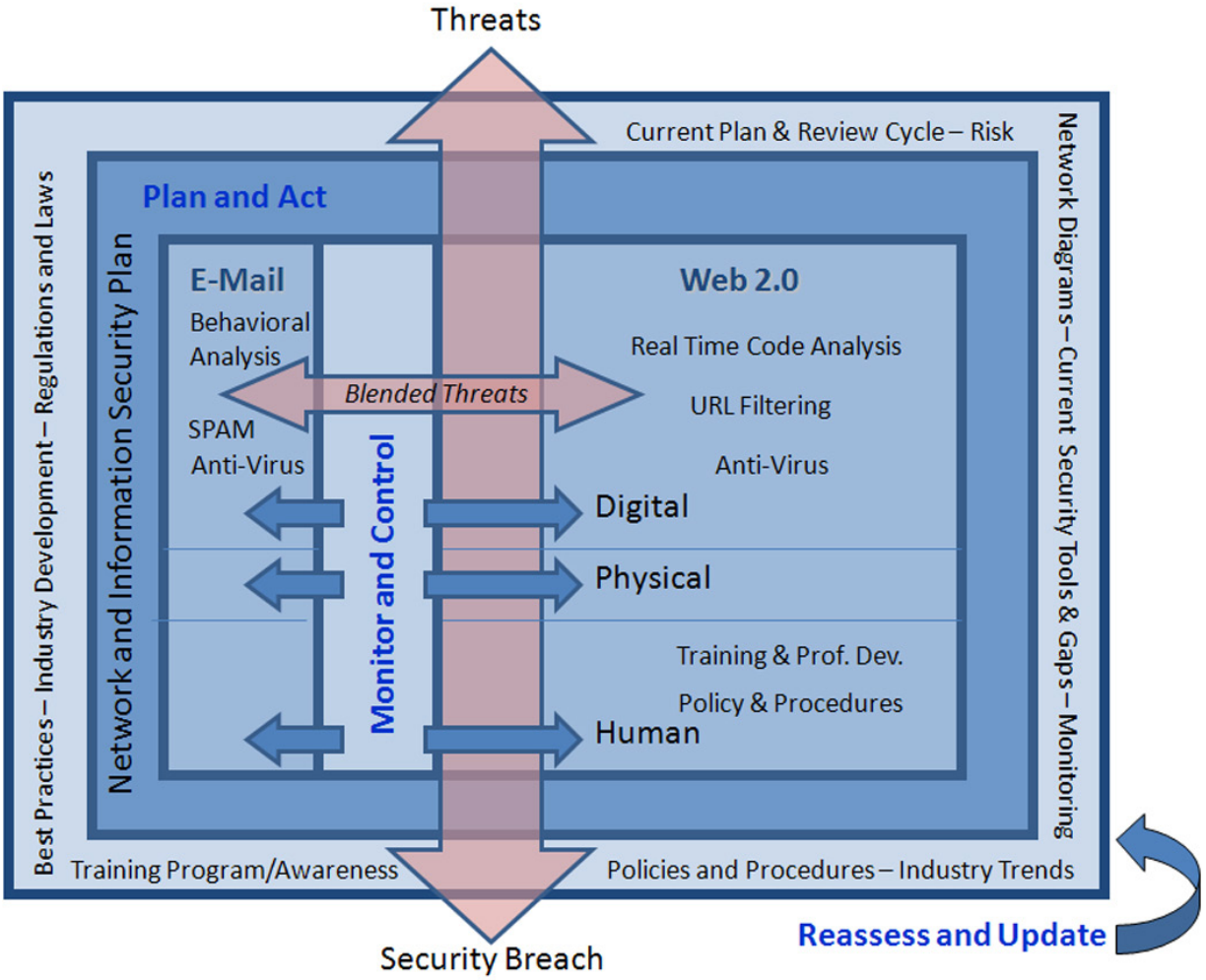

Figure 1 - Network and Information Security Model

Draft, Approve and Implement the Organization's Network and Information Security Plan (NISP)

Drafting of the plan begins with developing a formal **Understanding and Assessment** of the current status. This drives the development of the **Plan and Actions** to be executed. The plan should take a holistic view and address all layers of the Network and Information Security Model and clearly identify the risks associated and how these are being mitigated by the plan. Once drafted, seek formal approval from the organization and secure funding for implementation. As indicated, the approach to the modern cyber security plan must address Human, Physical, and Digital assets as detailed below.

The **Human Layer** protections are the behaviors and rules found at the foundation of the Network and Information Security Model. The sub-layers include Policies and Procedures as well as Training and Professional Development. This layer is necessary to address the critical human behaviors and raise awareness to the importance of network and information security in the organization. The policies addressed should at a minimum include these requirements:

- securing mobile client and information
- response to security incidents
- notification of security incidents
- work from home
- assignment of network access privileges
- individual accountability including password management
- intellectual property and safeguarding of protected information

In addition, this must include the implementation or modification of the organization's information technology change management process to include addressing the network and information security policies of the organization.

The **Physical Layer** protections include such things as building access control systems, surveillance systems, access to system consoles and equipment, equipment that is entering and exiting the buildings, i.e. the physical items that represent and are part of the organization's infrastructure. Protecting and planning physical security measures and how these are addressed in the network and information security plan must be considered.

The **Digital Layer** is where frequent change is often found. This is also where true creativity from both sides of the Threat Challenge (i.e. Hacker) and Response (i.e. Defender) occurs. This layer is where schools have deployed their digital defenses, i.e. Firewalls, Antivirus, and SPAM/URL Filtering solutions. Unfortunately the creativity of the hacker creates new and innovative ways of cracking through your digital defense. For example, today blended threats are common. This is a coordinated attack where a hacker leverages E-mail and the web to direct the unsuspecting victim to a malware-infused, hacked-yet-reputable website. The organization must turn to the digital security industry and trusted security solution partners to develop new and appropriate ways to combat these challenges. The appropriate solutions should be included in the security plan. At the Digital level E-mail and Web 2.0 are classified as content areas, however, with convergence more and more service areas must be included in the security plan with vulnerability assessment and protection measures put in place such as for building automation systems, Voice over IP, and video and surveillance systems.

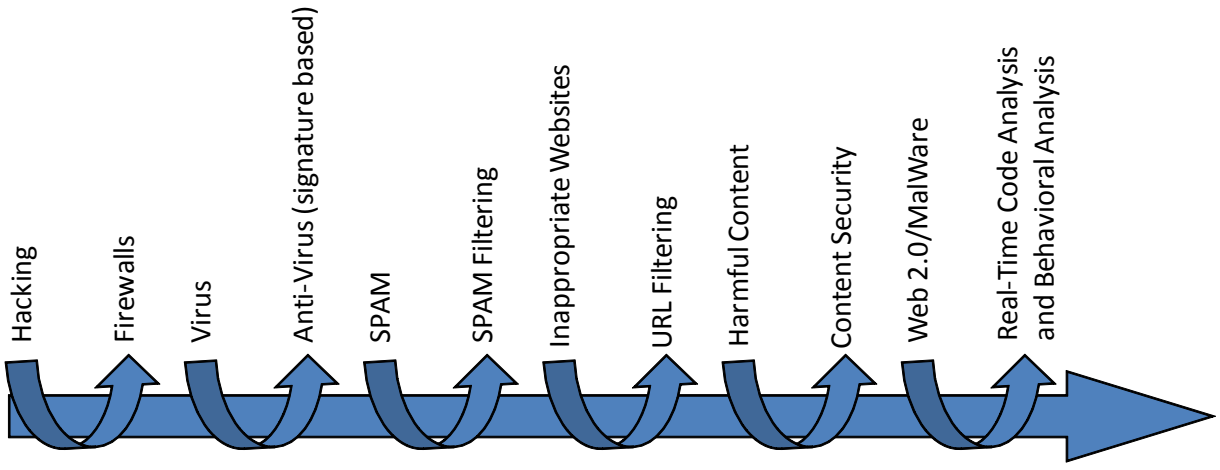

Figure 2 - Continuum of Threat Challenge and Response

As a part of this planning process, the **Monitoring and Control** considerations may be the most critical. The policies, processes, training, and tools put in place must provide the details, reports, and capability for security events to be viewed, understood, and acted on appropriately. The ability to respond to security events or potential security breaches with clear process and understanding for all users is critical to the security plan. Responding to threats as they penetrate deeper into the organization should be understood before the breach occurs. Establishing the "security dashboard" with specific and well-defined alerts, measures and reaction processes will enable the organization to measure its success or failure in deploying the network and information security plan.

Reassess and Update the Network and Information Security Plan (NISP)

The NISP is a living and breathing document that drives the network and information security decisions and behaviors of the organization. Therefore, the ongoing **Reassessment and Update** of the NISP is critically important. This is particularly true in the **Digital layer**, because the threat challenge and response cycle in this area can move very quickly. For example, emerging threats in the Web 2.0 area include rapid malware deployment and vulnerability where the victims are hit before the existing and currently deployed technology, i.e. signature based solutions, can react and protect. Add to this the fact that it could be some time before corrective application or operating system patches are made available and subsequently applied to vulnerable systems. This delay is known as the "window of vulnerability". These types of threats are commonly referred to as "zero-day" threats or exploits. Hackers are getting more sophisticated in how they deploy their attacks and are able to expose and take advantage of this weakness. The zero-day issue is growing as a percentage of all security incidents and this trend has created the need for new and innovative technology solutions to address it.

In addition, by breaking up malware code into small parts, i.e. mutated code, hackers have created a way to defeat the traditional signature based malware detection and removal solutions. Mutated malware, after passing through undetected by the signature based security protection measure, is reassembled to its original destructive form on the unsuspecting user's computer. To combat this threat, new and innovative real-time code analysis solutions are now available where the intent of a webpage is evaluated. Through real-time code analysis mutated malware threats can be detected and removed. Schools should consider a real-time code analysis technology as part of their regular NISP reassessment and update.

The mobility of the user is increasing and the security concerns around this trend are also emerging and must be soon addressed. As users move from place to place, network to network, organizations need to be able to monitor, manage, and protect the mobile user. More sophisticated "cloud-based" solutions are now being developed and made available to meet this need. These offer full-time vulnerability protection and policy management regardless of the user's location or the network to which they are connected.

In summary, network and information security is a vital concern for IT leaders, who must recognize the potential challenges and embrace a comprehensive, proactive strategy to protect their information, resources, and people. Providing this protection is a three-step process:

1. Create a role/position for a Network and Information Security Officer (NISO)
2. Draft, approve, and implement a Network and Information Security Plan (NISP) that addresses the Human, Physical and Digital layers and includes the following components:
   - Understand and Assess
   - Plan and Act
   - Monitor and Control
3. Reassess and continuously update the NISP

As educational organizations move into the future, the need for a comprehensive and continuous approach to addressing the network and information security remains a critical concern and on-going challenge. Safety and security within the digital world must be ensured for end users and mission critical information. IT leadership must embrace this responsibility and be prepared to protect and serve network citizens who put their faith and trust in the organization's ability to provide them with the leadership and information needed to be successful.

SECURITY FEATURES TO ADDRESS EMERGING ISSUES

M86 Security provides effective solutions to combat the current threats and issues facing education. A new generation of security solutions with M86 is here today that can help you meet your network and information security plan with confidence.

To combat the zero-day vulnerability and mutated malware, M86 offers technology that examines incoming and outgoing Web content and any embedded code is evaluated for its intent; this reduces the dependence for signatures and the hacker work-around to signature-based malware identification. This is accomplished with M86 Security's Patented Real-Time Code Analysis Technology. This real-time protection achieves the highest rate of malicious code prevention.

For email protection, M86 MailMarshal technology has a complete range of security features, including the Blended Threats module which stops the blended threat emails from even getting to users' inboxes by analyzing the embedded links in email messages with a cloud-based Behavioral Analysis service.

In addition, M86 offers consistent security and policy management for the mobile user through a combination of local and cloud based Real-Time Code Analysis Technology protection, extending security protection to the mobile user when on or off your network.

M86 Security provides multilayered security solutions for education to enable the end user with confidence and protection in the mobile Web 2.0 world. For more information, visit www.m86security.com.

CELT ACKNOWLEDGEMENT

This white paper was developed for M86 Security by the Center for Educational Leadership and Technology (www.celtcorp.com) located in Marlborough, Massachusetts. For nearly two decades, CELT has helped align leadership, learning, and technology in support of improved student achievement, by working collaboratively with educational organizations to support and transform teaching, learning, and administrative processes. CELT's mission is to help learning organizations attain their vision, mission, and goals by integrating high-quality programs, services, and technology with the organization's people and processes in a timely, efficient, and cost-effective way. For the past several years, CELT has been a leader in assessing and designing learner-centered, instructionally focused, and affordable decision support/accountability systems that are valid, reliable, and replicable at the student, classroom, school, school district, state, and federal levels. In addition to helping establish data definitions and systems and network architecture, CELT assists with the alignment of data systems with contemporary research, best practices, proven business processes, and governance policies.

Additional Resources

Inside the Jaws of Trojan.Clampi, September 25, 2009 - http://www.symantec.com/connect/blogs/inside-jaws-trojanclampi

Inside Trojan.Clampi: Network Communication, October 6, 2009 - http://www.symantec.com/connect/blogs/inside-trojanclampi-network-communication

School boards hit with cast-stealing Trojan, by Robert McMillan, 9/28/09 - http://www.computerworld.com/s/article/9138636/School_boards_hit_with_cash_stealing_Trojan

Guide for Developing Security Plans for Federal Information Systems, February 2006, Marianne Swanson, Joan Hash, Pauline Bowen. NIST Special Publication 800-18 Revision 1.

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH.

Security, Privacy and The Law, Posted at 11:00 AM on June 9, 2009 by Gabriel M. Helmer. Massachusetts Regulators Present on New Information Security Rules – June 5, 2009, Suffolk University Law School.

Guide for Developing Security Plans for Federal Information Systems, February 2006, Marianne Swanson, Joan Hash, Pauline Bowen. NIST Special Publication 800-18 Revision 1.

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH.

Security, Privacy and The Law, Posted at 11:00 AM on June 9, 2009 by Gabriel M. Helmer. Massachusetts Regulators Present on New Information Security Rules – June 5, 2009, Suffolk University Law School.

Citations

[1] New York District Faces $500,000 Loss in Cyber Bank Theft, By Dian Schaffhauser, 01/12/10 - http://thejournal.com/Articles/2010/01/12/New-York-District-Faces-500000-Loss-in-Cyber-Bank-Theft.aspx?Page=1

[2] eSchool News, October 1, 2009 Computer virus steals $325 from district, http://www.eschoolnews.com/2009/10/01/computer-virus-steals-325k-from-district/

[3] W. Pa. school district among targets of cyber-attacks, many originating in Europe, The Associated Press, 8/26/09 - http://pittsburghlive.com/x/pittsburghtrib/business/s_640015.html

[4] New York District Faces $500,000 Loss in Cyber Bank Theft, by Dian Schaffhauser, 1/12/10 - http://thejournal.com/Articles/2010/01/12/New-York-District-Faces-500000-Loss-in-Cyber-Bank-Theft.aspx?Page=1

[5] eSchool News, October 1, 2009 Computer virus steals $325 from district, http://www.eschoolnews.com/2009/10/01/computer-virus-steals-325k-from-district/

[6] New York District Faces $500,000 Loss in Cyber Bank Theft, by Dian Schaffhauser, 1/12/10 - http://thejournal.com/Articles/2010/01/12/New-York-District-Faces-500000-Loss-in-Cyber-Bank-Theft.aspx?Page=1

[7] Inside the Jaws of Trojan.Clampi, by Patrick Fitzgerald, 9/25/09 - http://www.symantec.com/connect/symantec-blogs/security-response/all/2009/09/all/en

[8] W. Pa. school district among targets of cyber-attacks, many originating in Europe, The Associated Press, 8/26/09 - http://pittsburghlive.com/x/pittsburghtrib/business/s_640015.html

[9] School district crippled by virus, by Dharm Makwana, 24Hours, 1/14/09 -http://vancouver.24hrs.ca/News/2009/01/14/8015156-sun.html

[10] Computer virus infects E. Providence, Chariho schools, by Alisha A. Pins, 5/15/09 - http://newsblog.projo.com/2009/05/computer-virus.html

[11] Hackers crack security on Eugene school employee info, by KVAL.co staff, 1/6/10 - http://www.kval.com/news/80827162.html

[12] M86 Security Labs Report: Closing the Vulnerability Window in Today's Web Environment - http://www.m86security.com/downloads

[13] Security threat report: July 2009 update, A look at the challenges ahead, Sophos, https://secure.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf

[14] Malware Statistics Update, Google Online Security Blog, August 25, 2009, Niels Provos, Anti-Malware Team, http://googleonlinesecurity.blogspot.com/2009/08/malware-statistics-update.html

[15] Kaspersky Security Bulletin 2009. Malware Evolution 2009, Eugene Aseev,s Alexander Gostev, Feb 17 2010, http://www.viruslist.com/en/analysis?pubid=204792101

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**

M86 SECURITY™

Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 03/1610