CYBER THREATS

AFFECTING MUNICIPALITIES TOO

Morris A. Enyeart, Ed.D.
City Connections LLC
91st Annual NJLM Conference

Cyber Threats

- What is a Cyber Threat?
- Inside vs Outside – Where is the greater danger?
- Are Municipal Web Sites a target?
- What is the Vendor’s Role?
- A Real Life Case

Cyber Threats – What are they?

Overt Threat – delivered electronically or by other means, identifies harm to persons, equipment, data, or a web site.

Cyber Threats – What are they?

Covert Threat – delivered secretly or disguised - viruses, worms, trojans, spam bots, identity theft, key loggers, etc.

The target is the municipality,
it is not an accident.

Remember to Report it as
you would any crime!

Cyber Threats – Inside vs Outside

The majority of Overt Threats come from INSIDE the municipality.

The majority of Covert Threats come from OUTSIDE the municipality.

Cyber Threats – Municipal Targets

YES – Municipalities Are A Target

- Disgruntled current or former employees.
- Political embarrassment.
- A vendor (outsourced or competitor)
- Someone seeking notoriety or to prove a point.
- Terrorist seeking to disrupt communications as part of a larger attack.
- Identity theft and phishing (credit cards)

Cyber Threats – A Vendor’s Role

- Advise and keep software up to date with patches and updates.
- Create and maintain logs of visitor traffic.
- Change passwords to admin accounts
- Keep a separate notification system for residents

Cyber Threats – Resources

- **http://www.us-cert.gov/** US-CERT (Computer Emergency Readiness)
- **http://www.dnsstuff.com/** for tracking the source of a threat.
- **http://network-tools.com/** Trace Route, firewalls, spyware removal and lots more.
- Report attacks to NJSP High Tech Crimes Unit

Cyber Threats – A Real Life Case

In October 2006 someone sent an email to a municipal police tip-line via their web site.

All they knew was what time the email was sent.

They called us to see what we could find out.

Cyber Threats – A Real Life Case

- **At 2:00pm the person used Google to get to the main police page.**
- 128.112.22.135 - - [20/Oct/2006:14:00:20 -0400] "GET /policemain.html HTTP/1.1" 200 5003 "http://www.google.com/search?hl=en&q=municipality+township+police" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
- **The person also accessed the tip line page at 2:00pm but did not use it to send a message.**
- 128.112.22.135 - - [20/Oct/2006:14:00:40 -0400] "GET /pt_tipline.html HTTP/1.1" 200 6159 "http://www.municipality.org/policemain.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
- **At 2:02 they accessed the tipline form.**
- 128.112.22.135 - - [20/Oct/2006:14:02:11 -0400] "GET /police_tipline_mail.html HTTP/1.1" 200 8441 "http://www.municipality.org/pt_tipline.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"

Cyber Threats – A Real Life Case

- **At 2:12 they clicked on the Submit button to send the message.**
- 128.112.22.135 - - [20/Oct/2006:14:12:26 -0400] "POST /cgi-bin/cgiemail/pttip.txt HTTP/1.1" 302 236 "http://www.municipality/police_tipline_mail.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
- **The person immediately received the thank you page which means the message was sent successfully.**
- 128.112.22.135 - - [20/Oct/2006:14:12:26 -0400] "GET /policethank.html HTTP/1.1" 200 4758 "http://www.municipality/police_tipline_mail.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"

Cyber Threats – A Real Life Case

- **From the thank you page they went to the Police Department telephone page.**
- 128.112.22.135 - - [20/Oct/2006:14:12:49 -0400] "GET /ptphone.html HTTP/1.1" 200 5151 "http://www.municipality/policethank.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
- **The person next went to the main police page.**
- 128.112.22.135 - - [20/Oct/2006:14:12:52 -0400] "GET /policemain.html HTTP/1.1" 200 5003 "http://www.municipality/ptphone.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
- particular PC. There is a name and phone number in the Whois record below.

Cyber Threats – A Real Life Case

- **The person next went to the Departments page.**

-
  ```
  128.112.22.135 - - [20/Oct/2006:14:12:55 -0400] "GET /departments.html HTTP/1.1" 200 10736 "http://www.municipality/policemain.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1; .NET CLR 1.1.4322)"
  ```
- **They then left the web site and have not accessed it again (at least not from that IP address),**
- The IP address 128.112.22.135 appears to come from XXXXXX. The following link will give you more information about source of the IP address. It is most likely sub-netted which means XXXXXX could probably pin it down to a particular PC. There is a name and phone number in the Whois record below.

Cyber Threats – Municipal Targets

Morris A. Enyeart, Ed.D.

City Connections LLC

www.cityconnections.com

888-534-8283