# Cyber Incident Response

# Are You Ready?

Ken Kuehni, CISSP, CISM, CRISC
ken.kuehni@ottawa.ca
613-580-2424 x23950

Mark Cunningham
mark.cunningham@ottawa.ca
613-580-2424 x20097

Senior Technology Security Analysts
City of Ottawa

[redacted]

IF IT HAPPENED TO THEM

IT COULD HAPPEN TO YOU

# Incident Response

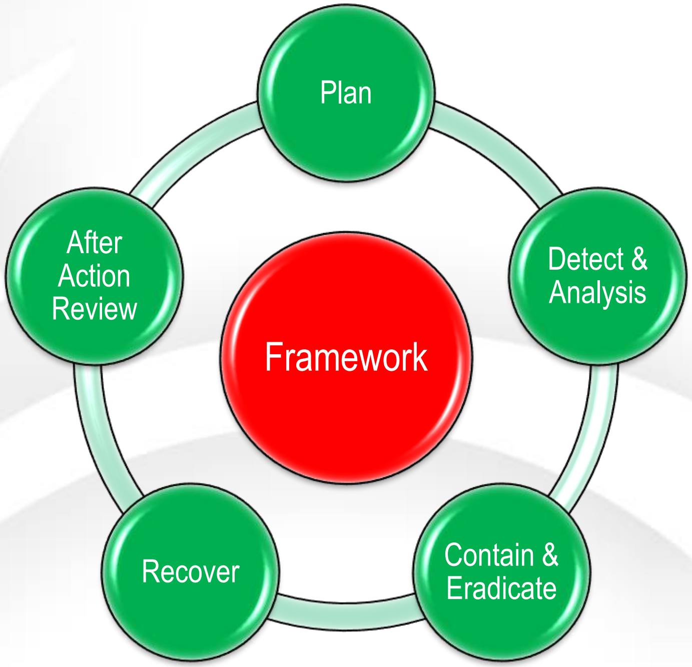
- Key components of a successful response capability
- Context of we applied it (Case Study)
- Lessons learned

# Common Language (NIST)

- **Event**
  - An observable occurrence (log entries)
- **Incident**
  - Violation or imminent threat  to Policies, Standards, or Security Practices
- **Breach**
  - Actual compromise of Confidentiality, Integrity, and/or Availability

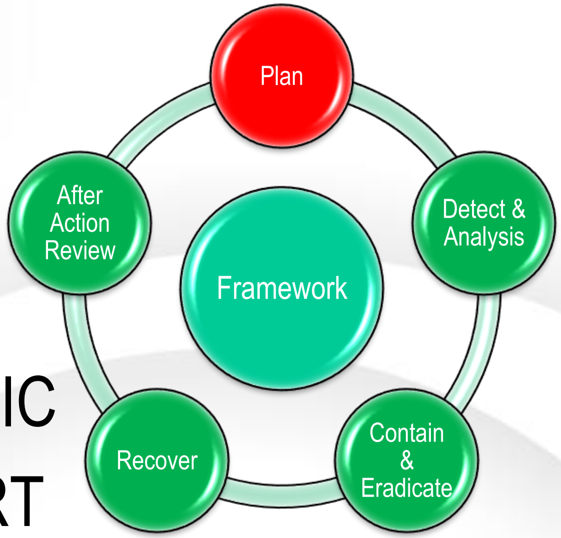
# What is Incident Response

- **Framework**
  - Corporate driven
    - Gives authority to the team
    - Supported (All levels of management)
    - Funded
  - Multiple phases
    - Right-size to your organization
    - It all starts with the Plan



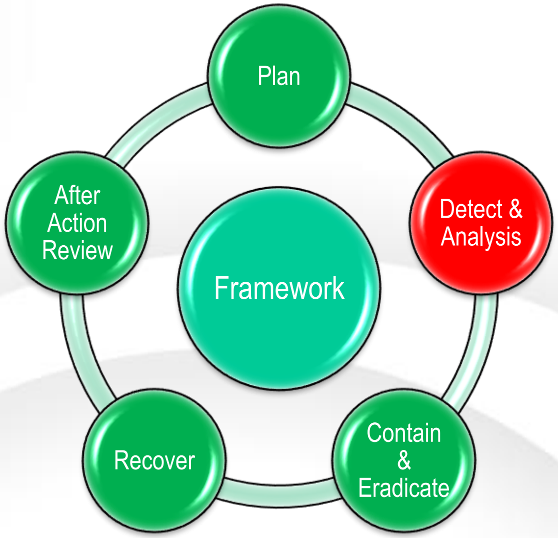
# Preparation

- **The Plan**
  - o Consistent methodology
  - o Alignment with BCP/DR
- **Resources- Right People**
  - o Not everyone is comfortable being an IC
  - o Identify Roles/People to build the CERT
- **Management Commitment**
  - o Day–to-Day stops
  - o Approve spending when required

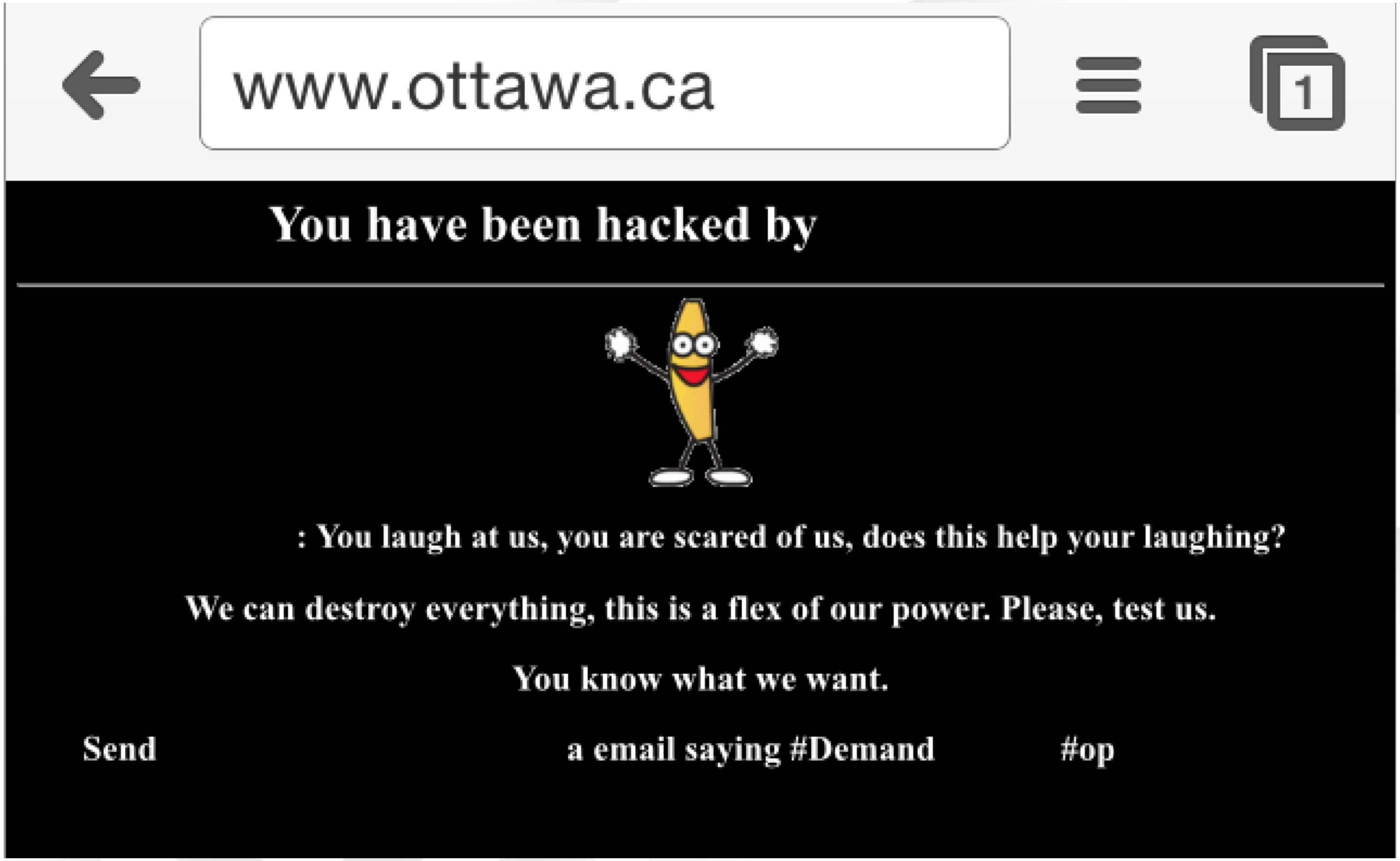


# Something Is Wrong

- **Detection & Analysis**
  - o 'Noisy'- things break, alerts triggered
  - o 'Stealthy'- time based/slow, evasive
  - o Understanding the attack
    - Vector, Actor, Targeted, Others
    - Size, Speed, Pivots, Impact levels
  - o Declaration
    - Activate the plan & Identify IC
    - Call in the CERT
    - Stand-up the Incident Command Center



# The Dancing Banana Case Study



www.ottawa.ca

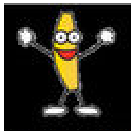
You have been hacked by

: You laugh at us, you are scared of us, does this help your laughing?

We can destroy everything, this is a flex of our power. Please, test us.

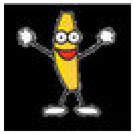
You know what we want.

Send a email saying #Demand #op



# The Perfect World

- It was a Friday evening around 17:30 hrs.
- I was out for dinner with a friend of mine
- A delicious meal had just been delivered to our table.
- Once finished the plan was to catch a movie.

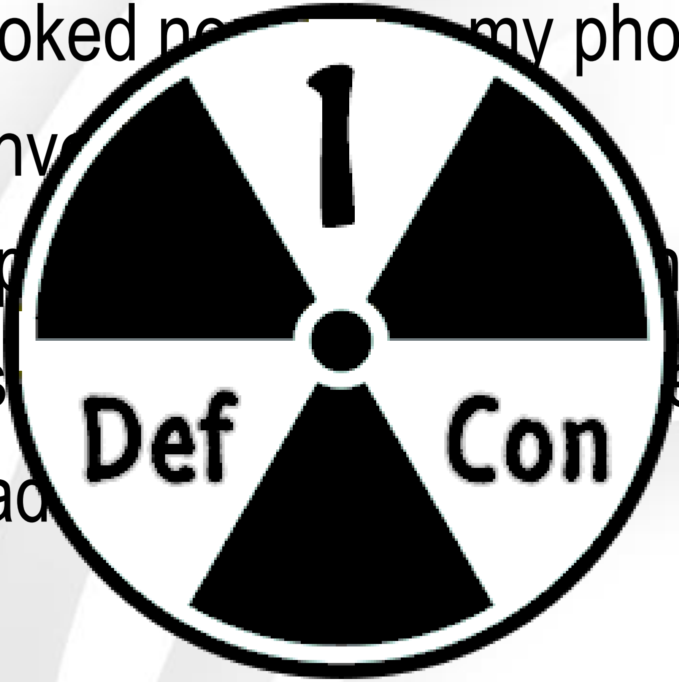


# The Real World

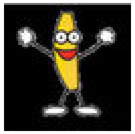
- It was a Friday evening around 17:30 hrs.
- I was out for dinner with a friend of mine
- A delicious meal had just been delivered to our table.
- I was On Call and received a notification that the City of Ottawa web page had been replaced with a dancing banana.

# The Real World (cont.)

- Ottawa.ca looked ne my phone
- Need more inv
- 2m later my p g nuts.
- News outlets en hacked.
- I knew we had

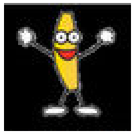


- **CHEQUE PLEASE!**



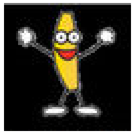
# Detection
## Friday, November 21, 2014
## 17:30 hrs

- City of Ottawa webpage was defaced by a hacktivist and replaced with a dancing banana with a message targeting Ottawa Police
- Media reports began circulating that the City's webpage had been hacked
- Confusion initially as the dancing banana web page was not visible across all Domain Name Servers



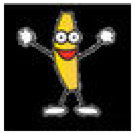
# Detection (cont.)

- Incident declared
- Establishment of a core response team
  - Incident commanders identified
  - Established leadership roles amongst various groups
    - Empowering people is key to a successful response
  - Ensure maximum shift duration is identified
- Incident log file started
  - This is the Incident Commanders lifeline



# Detection (cont.)

- Leveraged the Office of Emergency Management to help coordinate internal communications
- This gave us connectivity into all City departments to advise on the situation and keep them up to date.
- Had the confidence of senior leadership by ensuring continuous  status updates

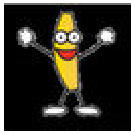


# Analysis

- Goal of hacktivist was to draw attention to a case in which a 16-year-old Ottawa teen was arrested for “swatting” by an Ottawa Police Officer

**Keep your eyes on the news (and social media)**

- The attacker was freely blogging on social media sites like twitter and actively engaged with the media



# Analysis (cont.)

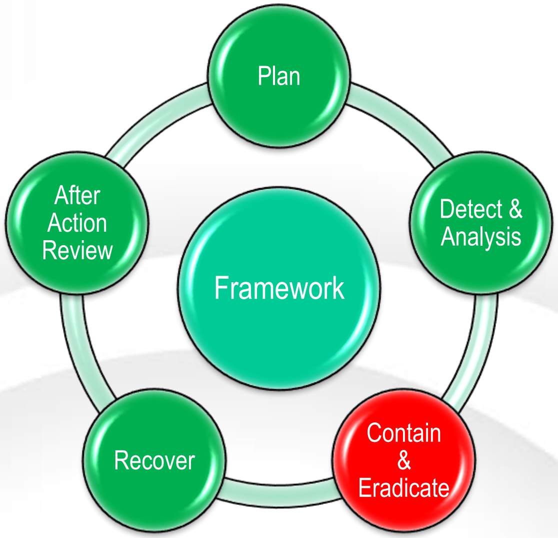
- Hacktivist social engineered the Domain Registrar and gained access to replace our domain name
- Our domain was redirected to a compromised server in the USA which was hosting the dancing banana

**Update the LOG**

- Keep your IR log up to date with EVERY piece of information you come across
- Make sure everything is dated and time stamped.

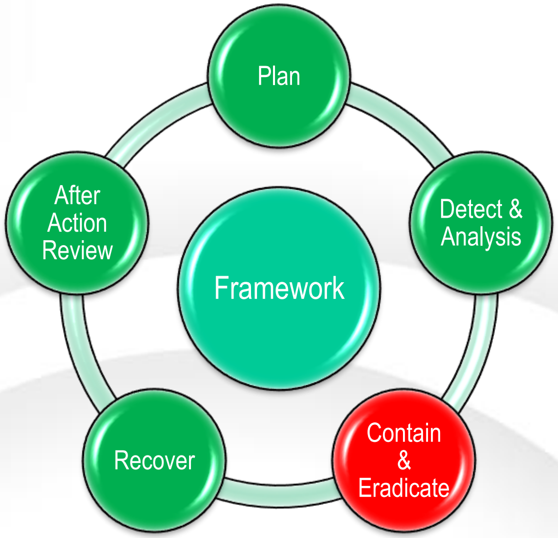
# Stopping the Damage

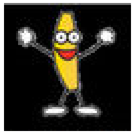
- **Containment**
  - o Enabling/Leverage controls
    - Perimeter controls (inbound/outbound)
    - Email filters
    - Patching systems
    - AV – fast track new definitions
    - Disable Macros, Ports



# Stopping the Damage

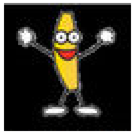
- **Eradication**
  - o Corrective actions
    - Malware removal
    - Remove compromised systems
    - Change passwords
    - Monitor for IoC's and update accordingly
  - o Considerations
    - Possible legal action – Forensic evidence, logs
    - Red Herrings, Parking Lot
    - SMEs are your experts





# Containment/Eradication

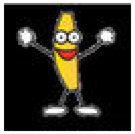
- Began the process of taking back control
- Identified the root cause and modified processes to tighten our security
- This was done in less than 2 hours



# Containment/Eradication

## Identify your Team Leads

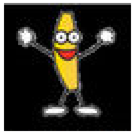
- We had various IR response leads working on specific areas of responsibility
  - Domain Registrar Team
  - Communications Team
  - Senior Management Lead



# Containment/Eradication (cont.)

**Ensure a consistent message is being distributed**

- The Communications IR lead assisted in the building of internal and public communications
- This ensured that the right message got out to all parties (Public and Staff)

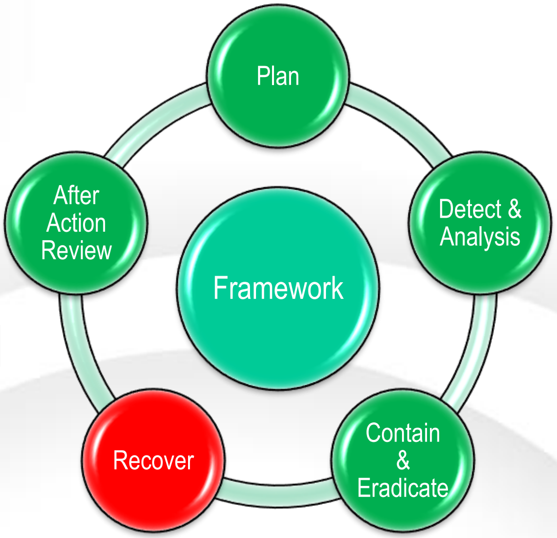


# Containment/Eradication (cont.)

- With successful containment we moved to the next phase
- Had the continued support of senior leadership by ensuring continuous status updates

# Getting Back to Normal

- **When to start**
  - It depends
    - Systems off line can be rebuilt
    - Restore resources (People, backups)
    - Are the same people containing that would be doing the restoring



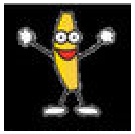
- **Who is back first**
  - BCP or DR may dictate
  - Consider impact to employees – Recovery could be big
  - External resources

# Recovery

**The road back to normal operations**

- The Dancing Ba [...] had a 24-48hr time to live clock at
- It took up to 2 [...] ttawa.ca domain name
  - o Established c [...] ver the time frame
  - o Maintained consta [...] senior leadership

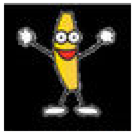
Monday, November 24, 2014
08:00 hrs



# Detection/Analysis
## Monday, November 24, 2014
## 08:00 hrs

**What’s up Doc?**

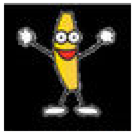
- The Ottawa.ca web page was unresponsive
- A large scale Distributed Denial of Service (DDoS) attack was occurring
- The attack was of a larger quantity than our technology safeguards could defend against
- The incident response cycle started again



# Detection/Analysis (cont.)

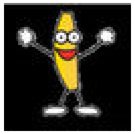
**Keep your eyes on the news (and social media)**

- The attacker was freely blogging AGAIN on social media sites like twitter and actively engaged with the media
- We were able to determine why this was happening



# Detection/Analysis (cont.)

- The media continued to bring the attackers name to the forefront
- This gives them all the power they need to continue
- As you will notice we do not reference the attackers name in our presentation
- The best thing you can do is take away their power by not being drawn into their game



# Containment/Eradication

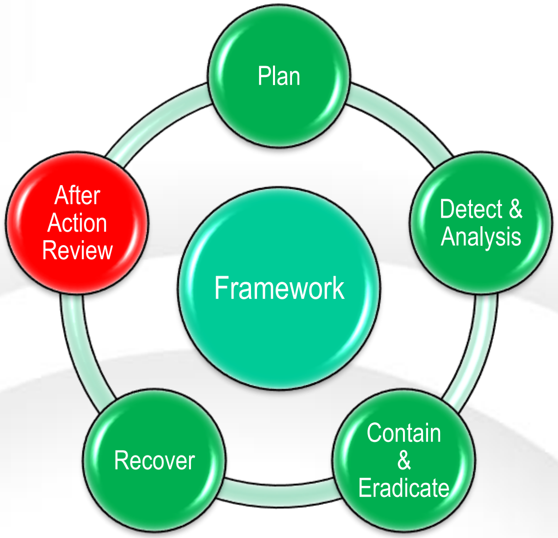
- Business decision was made to take Ottawa.ca offline
  - This lasted for 12hrs
- The response team implemented technical safeguards to defend against large scale DDoS attacks
- Worked with the Communications IR lead to ensure the public knew when we were back online

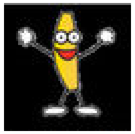
# Recovery

- Technical safeguard mplemented within 12hrs
- Ottawa.ca wa hrs Monday evening
- Continued atte e Ottawa.ca were observed b
- Continued attempts to breach our domain registrar were observed but unsuccessful

# Lessons Learned

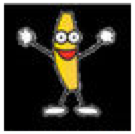
- **Incident wrap up**
  - Management Update
  - Standing Down
  - Post Actions
    - Corporate changes
    - Legal action, Law enforcement
- **Post incident review**
  - Team Brief
    - What worked well and what didn't
    - Plan Update





# Post Incident Review

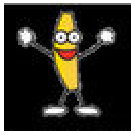
- Debrief was held within 48hrs
    - Try to hold he debrief within 72hrs
    - Hot washes are not always possible
- Identified what worked well
- Identified gaps, in our response plan
    - Always remember your people are working from the plan
    - When you look for gaps it is always with the plan, not the people



# Post Incident Review (cont.)

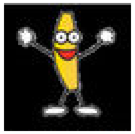
- Ensured people had an anonymous channel to provide feedback
  - Not everyone is comfortable speaking in public
  - You will get some really honest feedback this way
- Created an After Action Report with a list of recommendations to improve the response plan

# Reflection: An Incident Commanders Perspective



# Reflection: An Incident Commanders Perspective

- Maintain the Incident Log
  - This is your lifeline
- Keep your Senior Leaders update constantly
  - If they know what is happening they are less likely to keep asking you questions
- Promote staff to positions of leadership in the response chain
  - Giving people control over staff reduces the egos in the room



# Reflection: An Incident Commanders Perspective (cont.)

- Know what your people are doing
  - Take notes on what individuals are doing
  - Send out a note of thanks identifying 1 task that each individual did
  - It means a lot more than a generalized thank you note
- Make sure your senior leaders are aware of what these people did
  - Make sure you CC your people when you send it

# Key Components of the Plan

- Ensure an authority for declaring an incident has been identified
- Have roles identified and staff assigned to them
- Make sure communications people are identified
- Ensure maximum shift duration is identified

# Key Components of the Plan

- Have a standardized Incident Log
- Have a standardized debrief template
- Have a standardized After Action Report
- HAVE YOUR BOSS' PHONE NUMBER!!!!!
    - And all other contact information as well

# Key Take Aways for a Successful IR Methodology

- Gain Corporate Commitment
- Build the Plan
- Test the Plan <u>ANNUALLY</u>
- Update the Plan <u>ANNUALLY</u>

# Questions

???