Perkins, Gary CITZ:EX

From:	Perkins, Gary CITZ:EX
Sent:	May 11, 2018 5:37 PM
To:	George Pajari
Subject:	Re: Questions

Thanks for your help today!

Sent from my Samsung Galaxy smartphone.

-------- Original message --------
From: George Pajari <george.pajari@hootsuite.com>
Date: 2018-05-11 10:02 AM (GMT-08:00)
To: "Perkins, Gary CITZ:EX" <Gary.Perkins@gov.bc.ca>
Subject: Re: Questions

Shouldn't be a problem according to the UBC A/V person

If you have HDMI out we ought to be OK

On Fri, May 11, 2018 at 09:55 Perkins, Gary CITZ:EX <Gary.Perkins@gov.bc.ca> wrote:

> I don't want to be a nuisance but 2 questions
> 1. How bad will the slides look if not 16:9 and are 4:3
> 2. I haven't provided my presentation. Will using my PC be a problem?
>
> Sent from my Samsung Galaxy smartphone.

--
[Sent from my phone so apologies for brevity & typos.]

Perkins, Gary CITZ:EX

From: Perkins, Gary CITZ:EX
Sent: May 11, 2018 11:39 AM
To: beznosov@ece.ubc.ca
Subject: Re: invitation for keynote at UBC Cybersecurity Summit

Looking forward to presenting.

I did see this email but didn't have time to convert to 16:9. We will just work with it.

My slides are intended to be educational informative but emphasis on entertaining.

Finally I did let the AV guys know my laptop doesn't have HDMI but only VGA and miniDVI so we will be looking for an adapter.

Sent from my Samsung Galaxy smartphone.

-------- Original message --------
From: "Konstantin (Kosta) Beznosov" <beznosov@ece.ubc.ca>
Date: 2018-05-09 9:09 PM (GMT-08:00)
To: "Perkins, Gary CITZ:EX" <Gary.Perkins@gov.bc.ca>
Subject: Re: invitation for keynote at UBC Cybersecurity Summit

Hi Gary,

One more thing. The screen at the summit is naturally wide, so if you format your presentation slides for a wide screen (16:9 proportions), they will look the best.

See you on Monday!
Kosta
P.S. As of today, there 230+ registrations for the summit. So, we should have a full house.

On Fri, May 4, 2018 at 10:38 AM, Konstantin (Kosta) Beznosov <beznosov@ece.ubc.ca> wrote:

> Hi Gary,
>
> A couple of updates:
> - As of May 2, we had some 160 attendees registered for the summit and we expect more between then and May 7th, the last day of registration.
> - In case you want to take this into account in the preparation of your keynote, I'm sharing with you the talk info of the academic keynote, which will be given in the morning: http://blogs.ubc.ca/cybersecuritysummit/keynote-lujo-bauer/
>
> See you in a week!
>
> All the best,
> Kosta
>
> On Wed, Apr 11, 2018 at 8:59 PM, Konstantin (Kosta) Beznosov <beznosov@ece.ubc.ca> wrote:

Hi Gary,

Your keynote, including time for questions, will be 1 hour. So, you might want to keep your presentation to 45-50 minutes and leave 10-15 minutes for questions.

WRT topic, given the summit will be all about research in cybersecurity, it would be most interesting to hear your thoughts on the following points:
- What are the pressing cybersecurity problems in the public sector for which there are no ready solutions and which academic researchers can help with?
- How can public sector share data (including security & privacy incidents) with academic researchers in order to enable the researchers to investigate solutions to the above problems?
- How is public sector different and similar to private sector, when it comes to cybersecurity (including privacy)?

While these are my suggestions, I would totally understand it if you would prefer to re-use some of the presentation material that you have developed for other occasions. Just keep in mind that I expect the majority of Vancouver SecSIG to be there, and they might have seen some of your past presentations.

Whatever you decide on the content of your keynote, once you send me its title and abstract, I'll post them on the summit website.

I will ask video-streaming person not to do video/audio of your keynote. I presume it will be ok if the summit photographer will be making pictures of you during the keynote.

If your situation with the dinner on the 10th changes, please do let me know.

I took a note of your answers WRT other points.

All the best,
Kosta

On 04/10/18 11:02 PM, Perkins, Gary CITZ:EX wrote:

> Great! Thanks for following up, looking forward to it.
>
> 1. I am flexible on topic. What do you think would be of most interest? My gut is to go with some variation of “Getting to Defensible: Public Sector efforts to keep pace with the rapidly changing threat environment”. I am doing something for ISACA Vancouver that was to try to generate more attendance on Apr 26 - “2018 is the year of Cyberwar: 5 steps to surviving the apocalypse!” so a variation of that presentation would be the easiest.
>
> - cybersecurity briefing
> - cybersecurity threat landscape
> - critical infrastructure
> - incident response
> - role of government in security

- defensible security

2. I don’t expect to require expenses. I’m going to be in Vancouver the next week and so planning to come over earlier.

3. I prefer not to be filmed given my industry and I can be a lot more entertaining and candid that way with those who have joined.

4. Sounds good

5. Would like to attend but s.22 that week will likely not permit that.

6. I hope to stay for the whole thing. I know someone was looking to have me elsewhere during part of it but I’m going to do my best to remain there.

Let me know if you have any requests or know what people will get the most value out of.

I’m starting to think about a more patriotic approach, more inspirational.

Can you confirm – will be an hour and should leave 10 minutes for questions?

From: s.22 **On Behalf Of** Konstantin (Kosta) Beznosov
Sent: Tuesday, April 10, 2018 9:16 AM
To: Perkins, Gary CITZ:EX
Subject: Re: invitation for keynote at UBC Cybersecurity Summit

Hello, Gary,

The UBC Cybersecurity Summit is less than 5 weeks away and we are looking forward to your keynote. The venue holds up to 260 participants and the summit organizers are actively promoting the summit among local high-tech industry. Below are several important elements of your keynote that we need to arrange in advance:

1. We need your keynote title and abstract in the next week, so that we can advertise it on the summit website.

2. We have budget for your travel and lodging. Please make sure to keep your receipts and boarding passes, as you will need them for the expense claim.

3. We are arranging for the summit presentations, including your keynote, to be video-streamed and possibly archived for public viewing on YouTube. We'll be asking you to sign consent paperwork. If you will not give your consent, your keynote will not be streamed and will not be made available on YouTube. If you have to discuss it with your employer in advance, this is good time to do so.

4. The venue projector supports widescreen (16:9) presentations and you are encouraged to format your slides accordingly. If you are to choose to give your keynote using your laptop, an HDMI connection for your laptop will be provided. If you plan to include audio in your presentation, please do let me know in advance, so that we can do necessary adjustments to the video-streaming set-up.

5. If we arrange a pre-summit dinner with my colleagues from UBC and the other keynote speaker (and possibly representatives from the sponsoring organizations) in the evening of May 10, would you be interested in joining it?

6. We hope you can stay for the whole summit (8:30 AM - 6 PM). If you have to miss part of the summit, it would help for planning purposes to know about your plans for May 11.

All the best,

Kosta

On Thu, Nov 16, 2017 at 2:13 AM, Konstantin (Kosta) Beznosov <beznosov@ece.ubc.ca> wrote:

Hello, Gary,

Thank you for accepting this invitation and letting me know promptly. When, do you think, you will know your keynote will be approved on your side?

Can you please send me your headshot or a link to it, so that we can advertise your keynote on the summit website?

All the best,
Kosta

On 11/16/17 9:35 AM, Perkins, Gary CITZ:EX wrote:

Good evening,

Thanks for reaching out. I'd like to help, I am just in the process of arranging calendar for next year. Right now it doesn't look to conflict with anything. May 14-16 is the BCTech summit downtown so may work well.

I'd like to accept (pending any necessary approvals on this side and sorting out the calendar).

I hope all is well on your side.

Regards,

Gary Perkins

Executive Director, Chief Information Security Officer (CISO)

Information Security Branch

Office of the Chief Information Officer

Gary.Perkins@gov.bc.ca

250-387-7590

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. Any unauthorized copying, disclosure or distribution of the e-mail or the information it contains, is strictly forbidden.

From: Konstantin (Kosta) Beznosov [mailto:beznosov@ece.ubc.ca]
Sent: Wednesday, November 15, 2017 1:55 AM

To: Perkins, Gary CITZ:EX
Subject: invitation for keynote at UBC Cybersecurity Summit

Dear Gary,

I'm not sure if we officially met. I believe I saw you at the meeting organized by SERENE-RISC in Vancouver in April 2016.

At UBC, we are organizing a Cybersecurity Summit to be held on May 11, 2018, in Vancouver downtown. On behalf of the organizing and steering committees, I'd like to invite you to give an industry keynote at the summit.

Here's more information about your keynote and the summit:

- Your keynote will be about 1 hour, in the afternoon, likely 1:30-2:30 PM.
- You are encouraged to arrive to Vancouver the night before and attend the whole summit.
- While the budget for the summit does not allow us to offer any honorarium, we'll be happy to reimburse your travel and lodging expenses.
- We expect between 80 and 150 attendees, mostly from the local IT and high-tech industry.
- We plan to have an academia keynote in the morning.
- The topic of your keynote is up to you. We encourage you to take into account, if possible, the summit objectives, listed below, when you choose your keynote topic.

The objectives of organizing the summit are as follows:

1. Showcase to the local industry and to the members of the UBC community itself the UBC research related to the broad area of cybersecurity.
2. Help local cybersecurity industry and UBC researchers to connect.
3. Assess the potential for growing a more organized community of UBC faculty and graduate students doing research related to cybersecurity.

It will be the most helpful if you inform me by November 21 whether you accept this invitation.

All the best,
Kosta

--

```
_____________________________________________________________
 Konstantin Beznosov         http://www.ece.ubc.ca/~beznosov
 Professor

 Laboratory for Education and Research in Secure Systems
 Engineering                 http://lersse.ece.ubc.ca

 Department of Electrical and Computer Engineering
 University of British Columbia
 ____________________________________________________________
```

--

____

Konstantin Beznosov http://www.ece.ubc.ca/~beznosov

Professor

Laboratory for Education and Research in Secure Systems

Engineering http://lersse.ece.ubc.ca

Department of Electrical and Computer Engineering

University of British Columbia

____

--
____
Konstantin Beznosov http://www.ece.ubc.ca/~beznosov
Professor

Laboratory for Education and Research in Secure Systems
Engineering http://lersse.ece.ubc.ca

Department of Electrical and Computer Engineering
University of British Columbia
____

--
____

Konstantin Beznosov http://www.ece.ubc.ca/~beznosov
Professor

Laboratory for Education and Research in Secure Systems
Engineering http://lersse.ece.ubc.ca

Department of Electrical and Computer Engineering
University of British Columbia
____

From: Perkins, Gary CITZ:EX
Sent: May 6, 2018 1:07 PM
To: Perkins, Gary CITZ:EX
Subject: Fwd: invitation for keynote at UBC Cybersecurity Summit

Sent from my Samsung Galaxy smartphone.

-------- Original message --------
From: "Konstantin (Kosta) Beznosov" <beznosov@ece.ubc.ca>
Date: 2018-04-11 8:59 PM (GMT-08:00)
To: "Perkins, Gary CITZ:EX" <Gary.Perkins@gov.bc.ca>
Subject: Re: invitation for keynote at UBC Cybersecurity Summit

Hi Gary,

Your keynote, including time for questions, will be 1 hour. So, you might want to keep your presentation to 45-50 minutes and leave 10-15 minutes for questions.

WRT topic, given the summit will be all about research in cybersecurity, it would be most interesting to hear your thoughts on the following points:
- What are the pressing cybersecurity problems in the public sector for which there are no ready solutions and which academic researchers can help with?
- How can public sector share data (including security & privacy incidents) with academic researchers in order to enable the researchers to investigate solutions to the above problems?
- How is public sector different and similar to private sector, when it comes to cybersecurity (including privacy)?

While these are my suggestions, I would totally understand it if you would prefer to re-use some of the presentation material that you have developed for other occasions. Just keep in mind that I expect the majority of Vancouver SecSIG to be there, and they might have seen some of your past presentations.

Whatever you decide on the content of your keynote, once you send me its title and abstract, I'll post them on the summit website.

I will ask video-streaming person not to do video/audio of your keynote. I presume it will be ok if the summit photographer will be making pictures of you during the keynote.

If your situation with the dinner on the 10th changes, please do let me know.

I took a note of your answers WRT other points.

All the best,
Kosta

On 04/10/18 11:02 PM, Perkins, Gary CITZ:EX wrote:

Great! Thanks for following up, looking forward to it.

1. I am flexible on topic. What do you think would be of most interest? My gut is to go with some variation of "Getting to Defensible: Public Sector efforts to keep pace with the rapidly changing threat environment". I am doing something for ISACA Vancouver that was to try to generate more attendance on Apr 26 - "2018 is the year of Cyberwar: 5 steps to surviving the apocalypse!" so a variation of that presentation would be the easiest.
   - cybersecurity briefing
   - cybersecurity threat landscape
   - critical infrastructure
   - incident response
   - role of government in security
   - defensible security
2. I don't expect to require expenses. I'm going to be in Vancouver the next week and so planning to come over earlier.
3. I prefer not to be filmed given my industry and I can be a lot more entertaining and candid that way with those who have joined.
4. Sounds good
5. Would like to attend but s.22 that week will likely not permit that.
6. I hope to stay for the whole thing. I know someone was looking to have me elsewhere during part of it but I'm going to do my best to remain there.

Let me know if you have any requests or know what people will get the most value out of.
I'm starting to think about a more patriotic approach, more inspirational.
Can you confirm – will be an hour and should leave 10 minutes for questions?

From: s.22] **On Behalf Of** Konstantin (Kosta) Beznosov
Sent: Tuesday, April 10, 2018 9:16 AM
To: Perkins, Gary CITZ:EX
Subject: Re: invitation for keynote at UBC Cybersecurity Summit

Hello, Gary,

The UBC Cybersecurity Summit is less than 5 weeks away and we are looking forward to your keynote. The venue holds up to 260 participants and the summit organizers are actively promoting the summit among local high-tech industry. Below are several important elements of your keynote that we need to arrange in advance:

1. We need your keynote title and abstract in the next week, so that we can advertise it on the summit website.

2. We have budget for your travel and lodging. Please make sure to keep your receipts and boarding passes, as you will need them for the expense claim.

3. We are arranging for the summit presentations, including your keynote, to be video-streamed and possibly archived for public viewing on YouTube. We'll be asking you to sign consent

paperwork. If you will not give your consent, your keynote will not be streamed and will not be made available on YouTube. If you have to discuss it with your employer in advance, this is good time to do so.

4. The venue projector supports widescreen (16:9) presentations and you are encouraged to format your slides accordingly. If you are to choose to give your keynote using your laptop, an HDMI connection for your laptop will be provided. If you plan to include audio in your presentation, please do let me know in advance, so that we can do necessary adjustments to the video-streaming set-up.

5. If we arrange a pre-summit dinner with my colleagues from UBC and the other keynote speaker (and possibly representatives from the sponsoring organizations) in the evening of May 10, would you be interested in joining it?

6. We hope you can stay for the whole summit (8:30 AM - 6 PM). If you have to miss part of the summit, it would help for planning purposes to know about your plans for May 11.

All the best,
Kosta

On Thu, Nov 16, 2017 at 2:13 AM, Konstantin (Kosta) Beznosov <beznosov@ece.ubc.ca> wrote:
Hello, Gary,

Thank you for accepting this invitation and letting me know promptly. When, do you think, you will know your keynote will be approved on your side?

Can you please send me your headshot or a link to it, so that we can advertise your keynote on the summit website?

All the best,
Kosta

On 11/16/17 9:35 AM, Perkins, Gary CITZ:EX wrote:

> Good evening,
>
> Thanks for reaching out. I'd like to help, I am just in the process of arranging calendar for next year. Right now it doesn't look to conflict with anything. May 14-16 is the BCTech summit downtown so may work well.
>
> I'd like to accept (pending any necessary approvals on this side and sorting out the calendar).
>
> I hope all is well on your side.
>
> Regards,
>
> **Gary Perkins**
> Executive Director, Chief Information Security Officer (CISO)
> Information Security Branch

Office of the Chief Information Officer
Gary.Perkins@gov.bc.ca
250-387-7590

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. Any unauthorized copying, disclosure or distribution of the e-mail or the information it contains, is strictly forbidden.

From: Konstantin (Kosta) Beznosov [mailto:beznosov@ece.ubc.ca]
Sent: Wednesday, November 15, 2017 1:55 AM
To: Perkins, Gary CITZ:EX
Subject: invitation for keynote at UBC Cybersecurity Summit

Dear Gary,

I'm not sure if we officially met. I believe I saw you at the meeting organized by SERENE-RISC in Vancouver in April 2016.

At UBC, we are organizing a Cybersecurity Summit to be held on May 11, 2018, in Vancouver downtown. On behalf of the organizing and steering committees, I'd like to invite you to give an industry keynote at the summit.

Here's more information about your keynote and the summit:

- Your keynote will be about 1 hour, in the afternoon, likely 1:30-2:30 PM.
- You are encouraged to arrive to Vancouver the night before and attend the whole summit.
- While the budget for the summit does not allow us to offer any honorarium, we'll be happy to reimburse your travel and lodging expenses.
- We expect between 80 and 150 attendees, mostly from the local IT and high-tech industry.
- We plan to have an academia keynote in the morning.
- The topic of your keynote is up to you. We encourage you to take into account, if possible, the summit objectives, listed below, when you choose your keynote topic.

The objectives of organizing the summit are as follows:

1. Showcase to the local industry and to the members of the UBC community itself the UBC research related to the broad area of cybersecurity.
2. Help local cybersecurity industry and UBC researchers to connect.
3. Assess the potential for growing a more organized community of UBC faculty and graduate students doing research related to cybersecurity.

It will be the most helpful if you inform me by November 21 whether you accept this invitation.

All the best,
Kosta

--

Konstantin Beznosov http://www.ece.ubc.ca/~beznosov
Professor

Laboratory for Education and Research in Secure Systems
Engineering http://lersse.ece.ubc.ca

Department of Electrical and Computer Engineering
University of British Columbia

--

Konstantin Beznosov http://www.ece.ubc.ca/~beznosov
Professor

Laboratory for Education and Research in Secure Systems
Engineering http://lersse.ece.ubc.ca

Department of Electrical and Computer Engineering
University of British Columbia

Page 1

Withheld pursuant to/removed as

s.3

From: Konstantin Beznosov <beznosov@ece.ubc.ca>
Sent: May 11, 2018 11:39 AM
To: Perkins, Gary CITZ:EX
Subject: Autoreply Re: Re: invitation for keynote at UBC Cybersecurity Summit

Hello,

This is an automated response to your message regarding "Re: invitation for keynote at UBC Cybersecurity Summit".

Please note that, I am at UBC Cybersecurity Summit on May 11 and won't be able to handle your message(s). If it's urgent, please text me at s.22

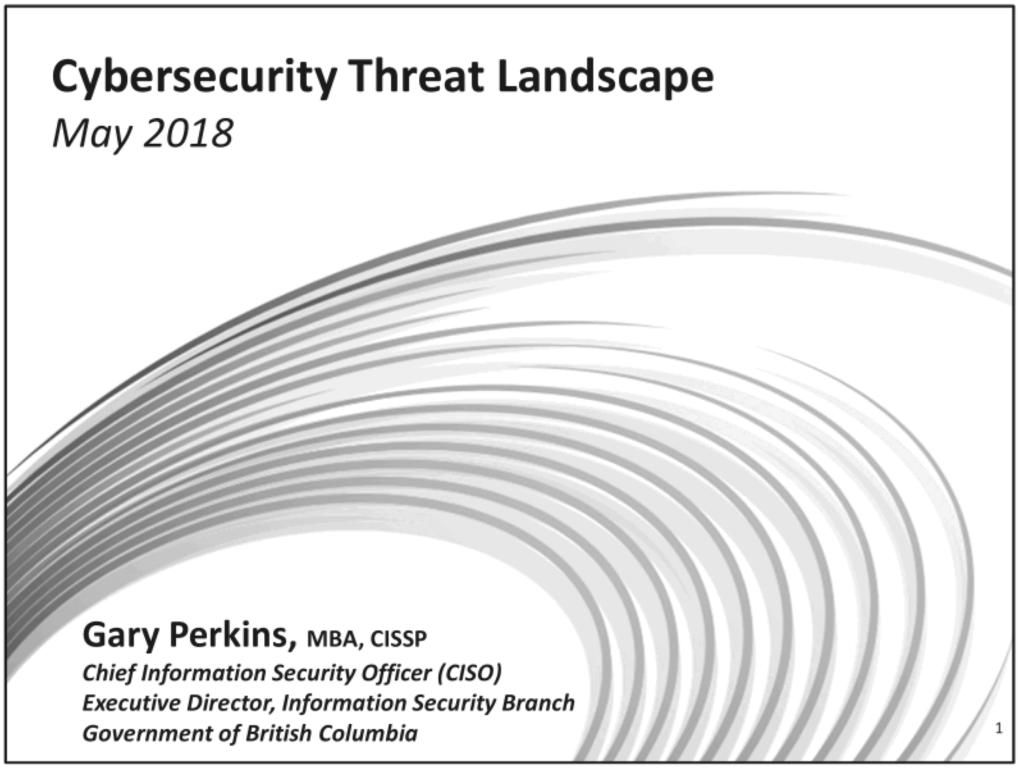
Thank you,
Konstantin

____

Konstantin Beznosov Professor
Electrical and Computer Engineering
University of British Columbia

http://www.ece.ubc.ca/~beznosov/

____

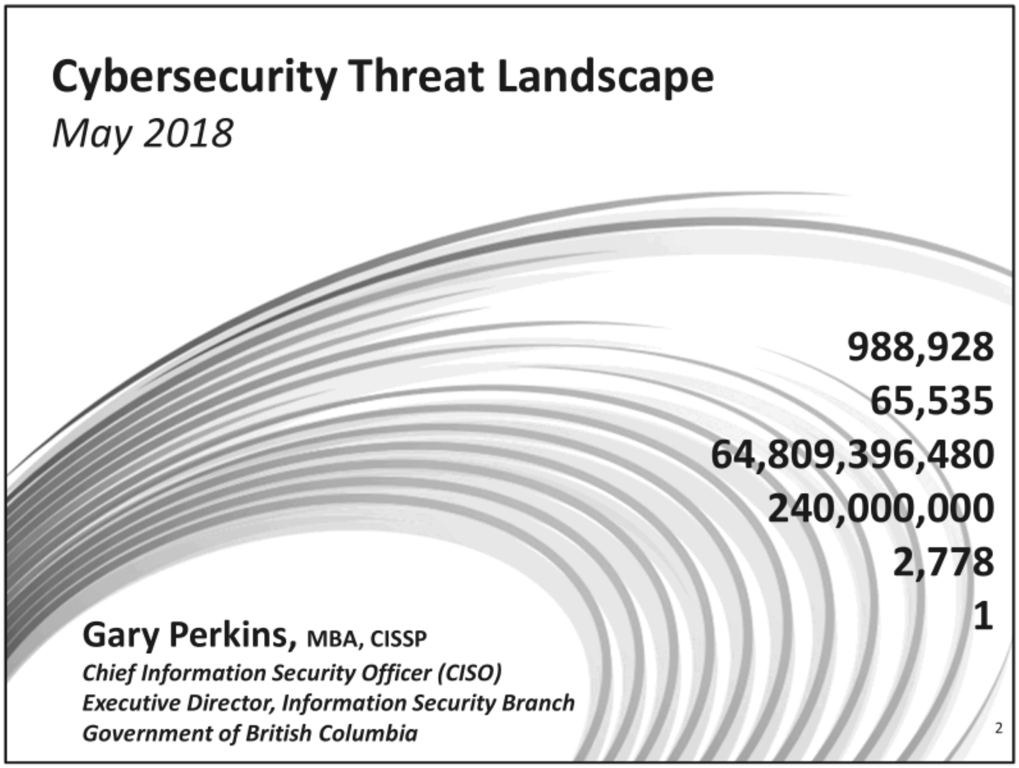


Cybersecurity Threat Landscape

May 2018

Gary Perkins, MBA, CISSP

Chief Information Security Officer (CISO)
Executive Director, Information Security Branch
Government of British Columbia



Cybersecurity Threat Landscape

May 2018

988,928
65,535
64,809,396,480
240,000,000
2,778
1

Gary Perkins, MBA, CISSP
Chief Information Security Officer (CISO)
Executive Director, Information Security Branch
Government of British Columbia

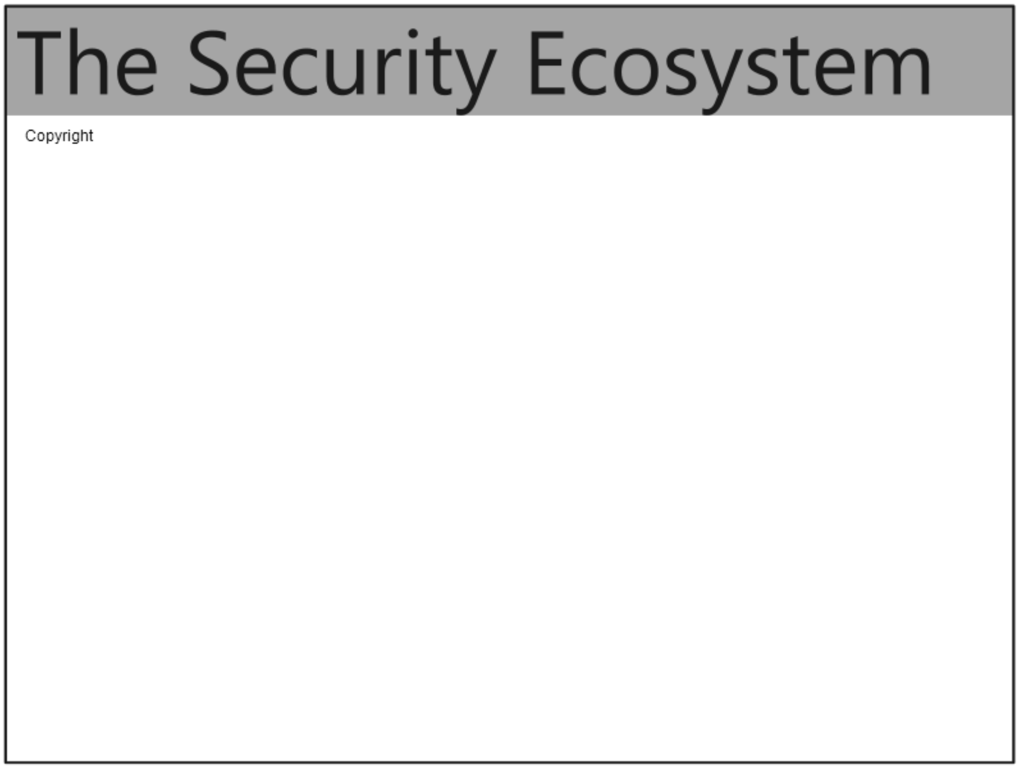
Copyright

Gary & Rob

Copyright

Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

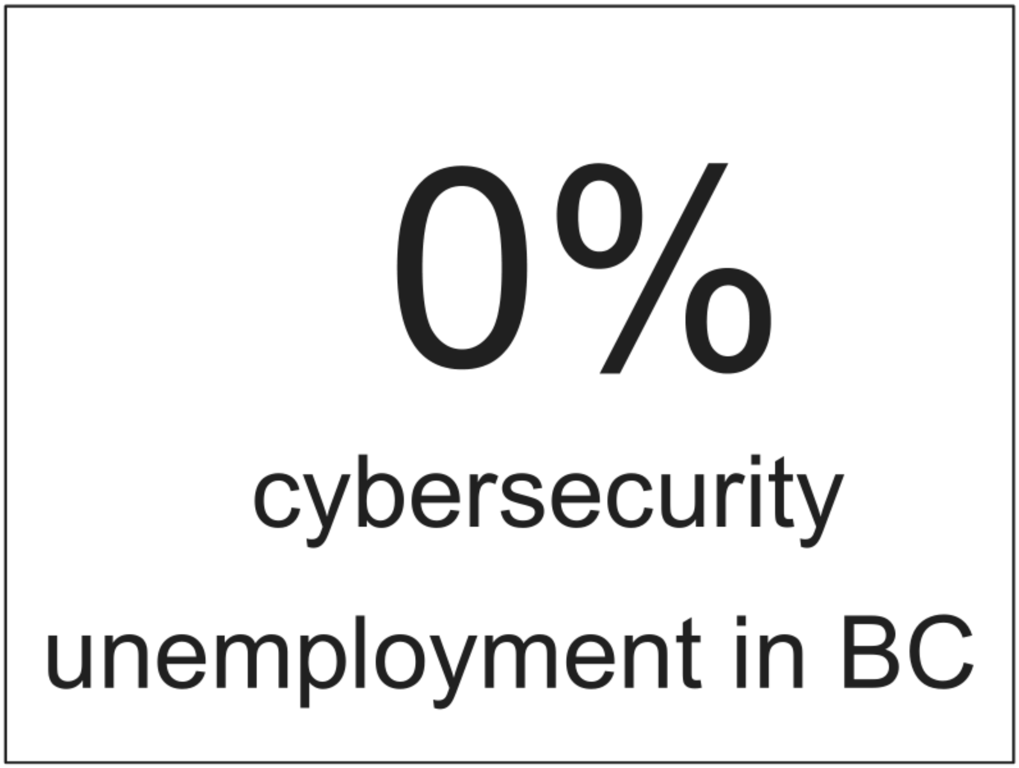
Gary



The Security Ecosystem

Copyright

Gary



0%

cybersecurity unemployment in BC

Gary & Rob

Copyright

SOURCES: **1.** *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015.* **9.** *State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

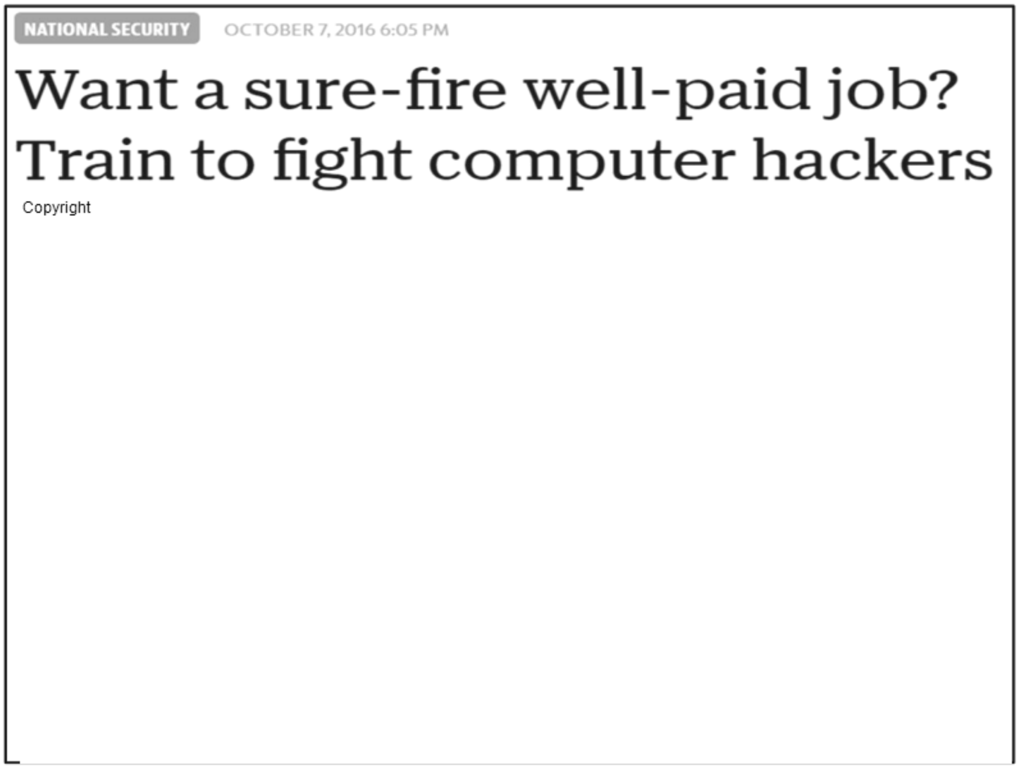
** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

https://cybersecurity.isaca.org

January 2016

One Million Cybersecurity Job Openings In 2016

Copyright

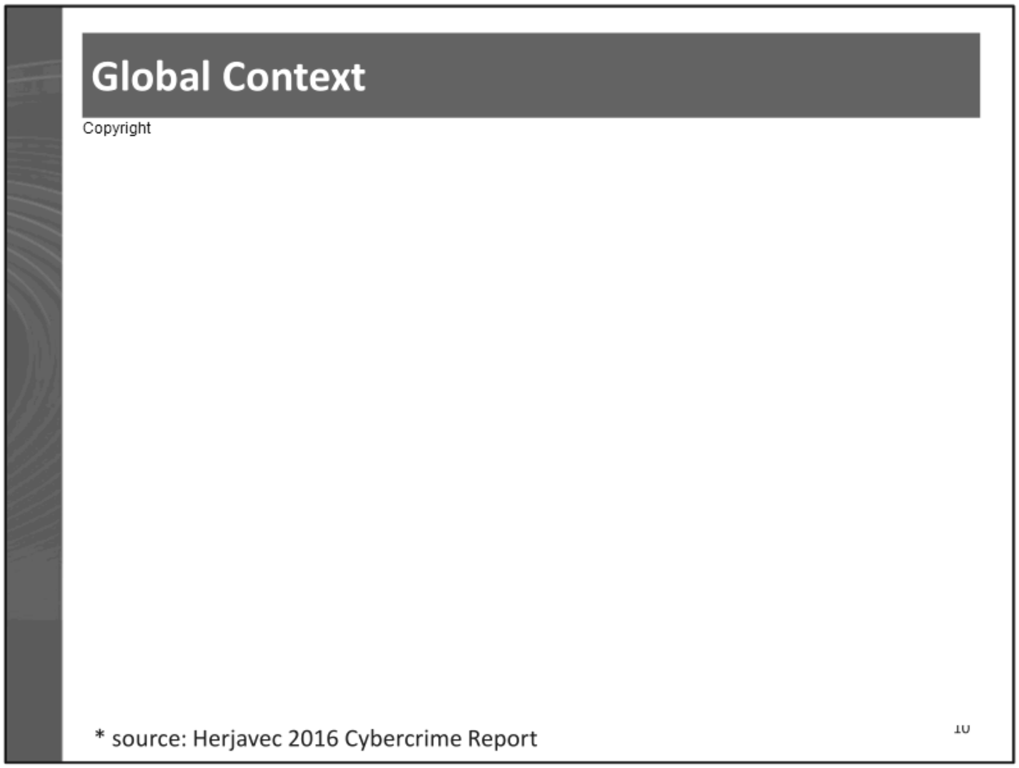


NATIONAL SECURITY OCTOBER 7, 2016 6:05 PM

Want a sure-fire well-paid job? Train to fight computer hackers

Copyright

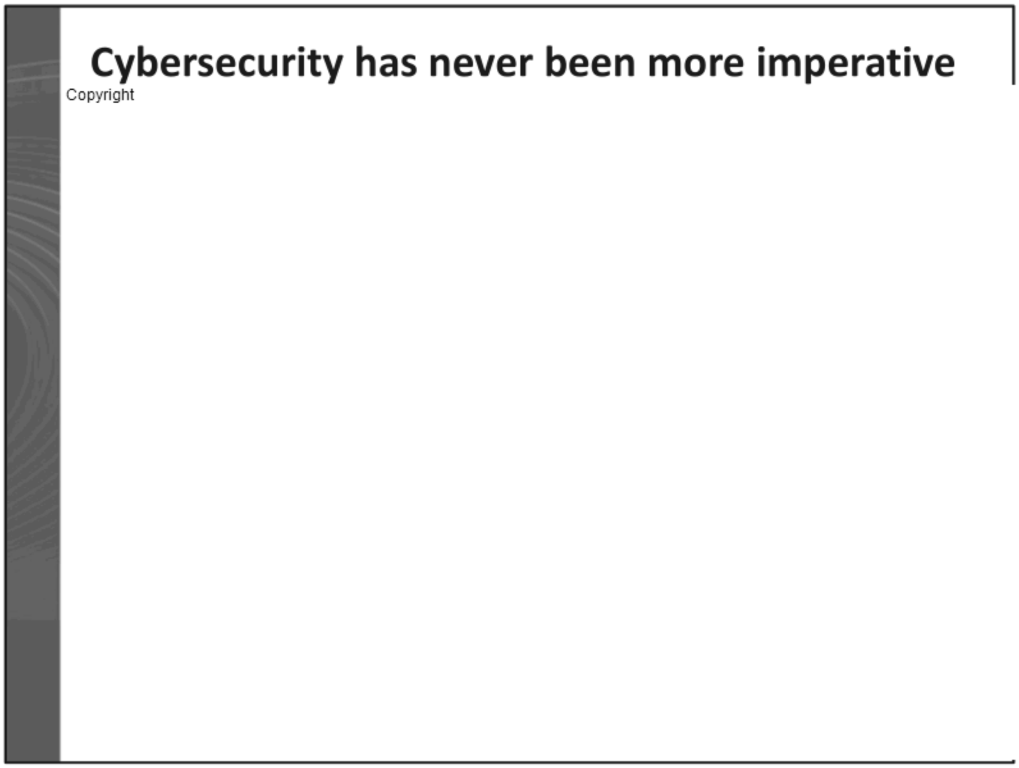
Gary



Global Context

Copyright

* source: Herjavec 2016 Cybercrime Report



Cybersecurity has never been more imperative

Copyright

2018 will be the year of cyberwar

The cyberattacks of the past year can only hint at the coming weaponization of security flaws Copyright

Justin Ling

December 25, 2017

Copyright

Copyright

www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16357&view=map

Digital Attack Map Top daily DDoS attacks worldwide

Copyright

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 5th Feb 2015)

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Copyright

Cybercrime costing U.S. billions; China to blame for most attacks: FBI chief

AFP-JIJI

Copyright

Topic: Government US

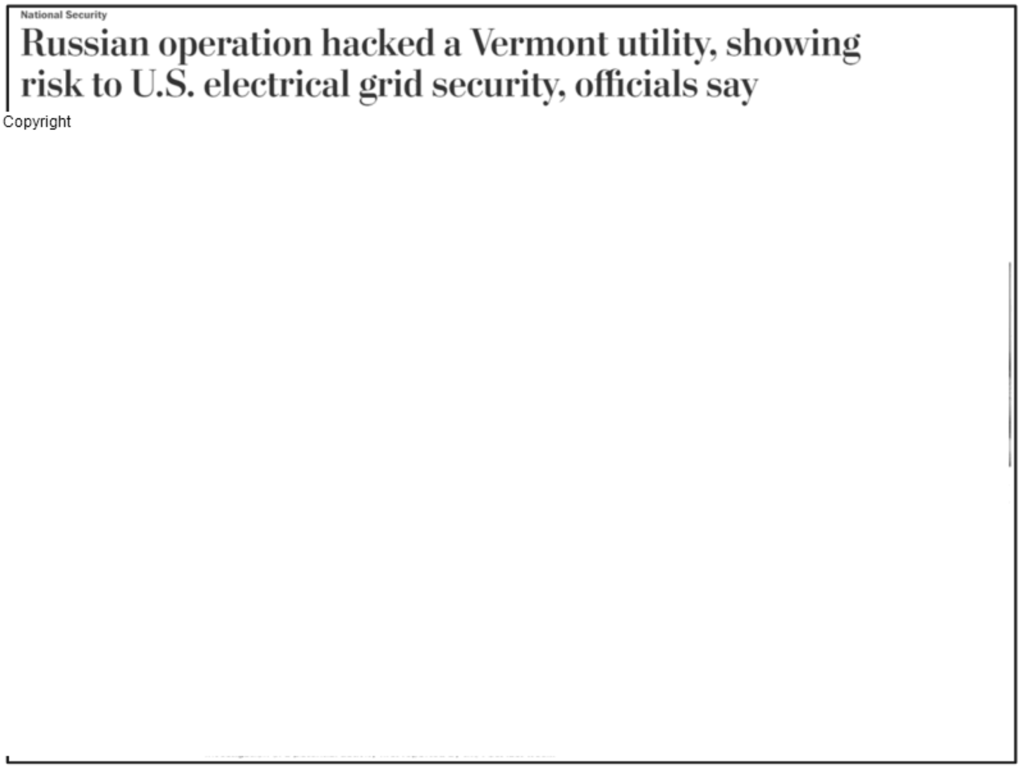
Follow via:

Richard Clarke: China has hacked every major US company

Copyright

US officially accuses Russia of hacking DNC and interfering with election

Copyright



National Security

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say

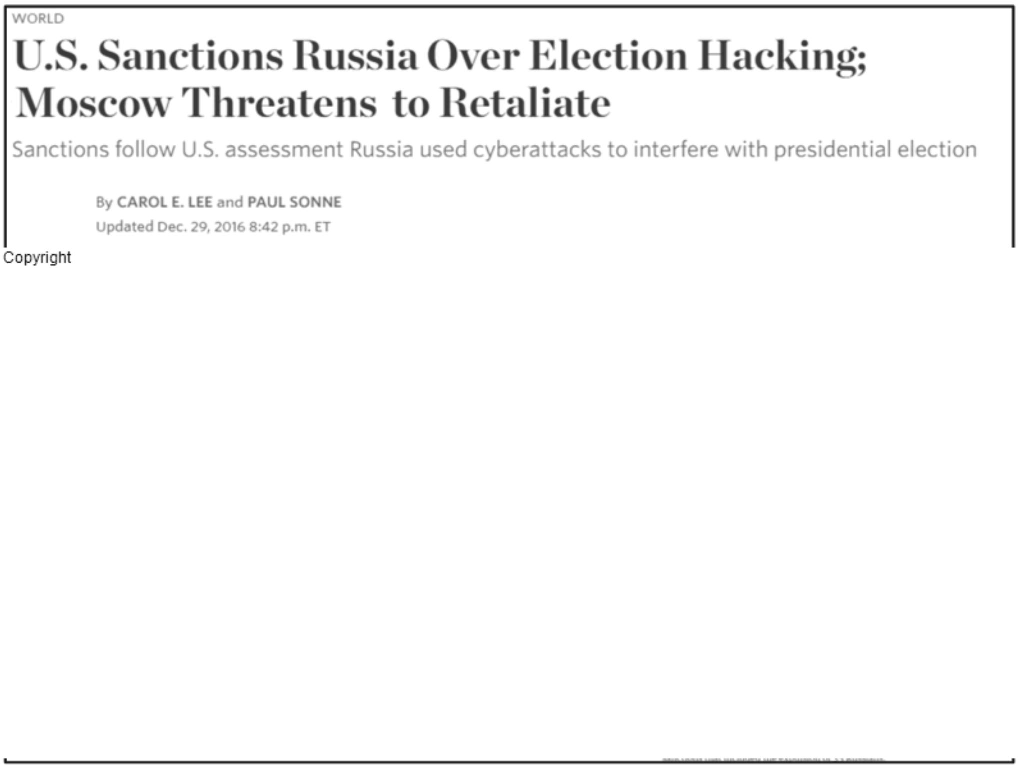
Copyright

Hydro-1 linked to hack of Vermont utility

Copyright

Police investigating possible cyber threat against Hydro One

Copyright



WORLD

U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate

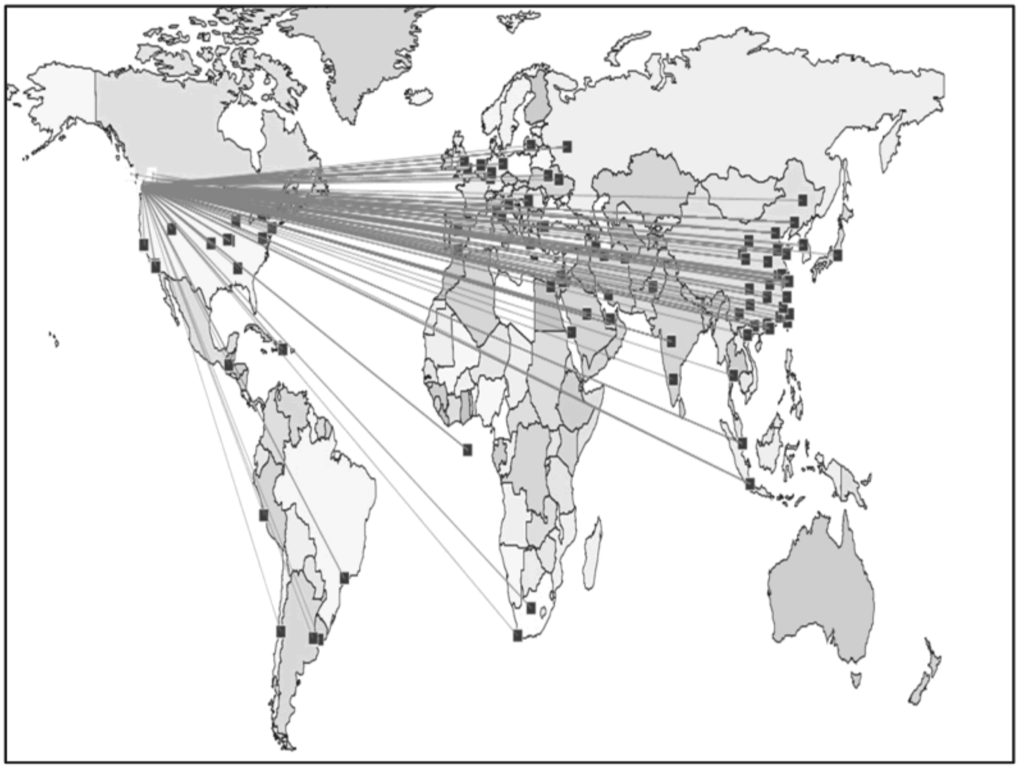
Sanctions follow U.S. assessment Russia used cyberattacks to interfere with presidential election

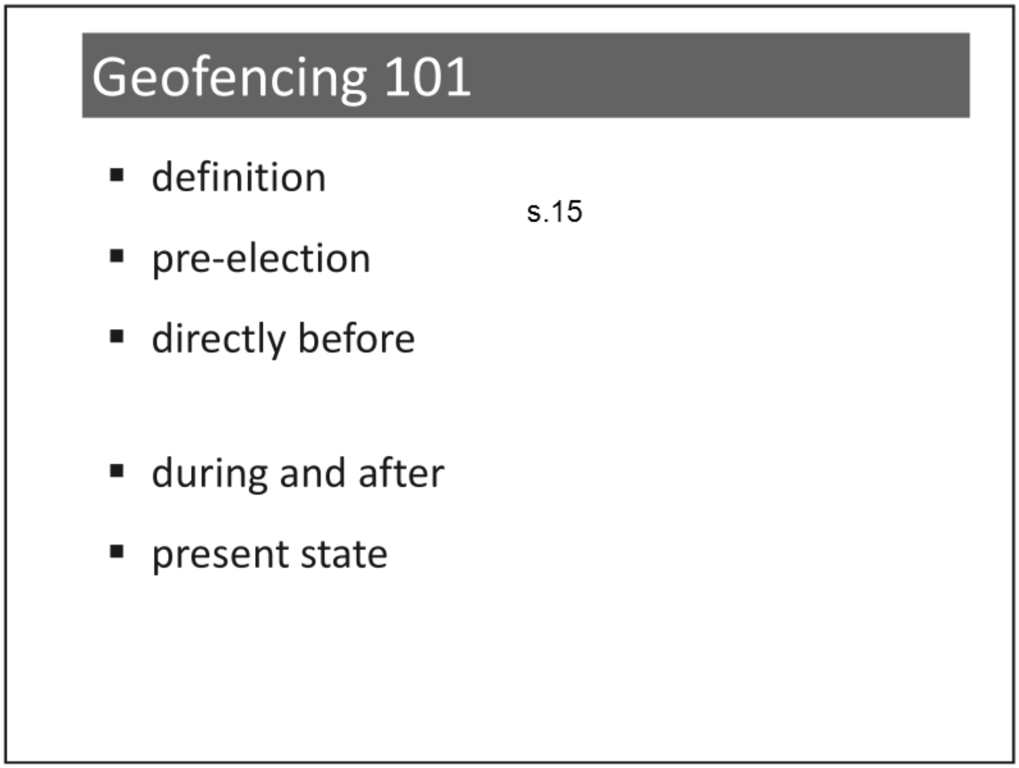
By CAROL E. LEE and PAUL SONNE
Updated Dec. 29, 2016 8:42 p.m. ET

Copyright

Cyber Threats to Canada’s Democratic Process

Copyright

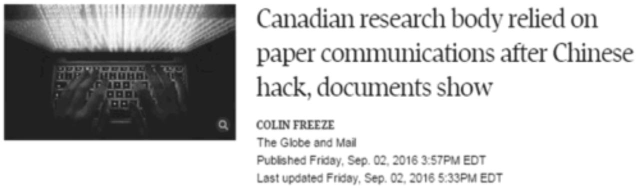




Geofencing 101

- definition
- pre-election
- directly before
- during and after
- present state

s.15



Canadian research body relied on paper communications after Chinese hack, documents show

COLIN FREEZE
The Globe and Mail
Published Friday, Sep. 02, 2016 3:57PM EDT
Last updated Friday, Sep. 02, 2016 5:33PM EDT

Copyright

Copyright

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Doctors reverted to pens and paper after hospital taken offline by a ransomware attack

By Lauren O'Neil, CBC News Posted: Feb 16, 2016 10:59 PM ET | Last Updated: Feb 17, 2016 10:03 PM ET

Copyright

University Of Calgary Paid $20,000 In Ransom To Hackers

The Huffington Post Alberta | By Sarah Rieger

Posted: 06/07/2016 5:53 pm EDT | Updated: 06/07/2016 5:59 pm EDT

Copyright

$10 SWITCHES COST BANGLADESH'S CENTRAL BANK $81 MILLION

By Lulu Chang — April 23, 2016 10:15 AM

Copyright

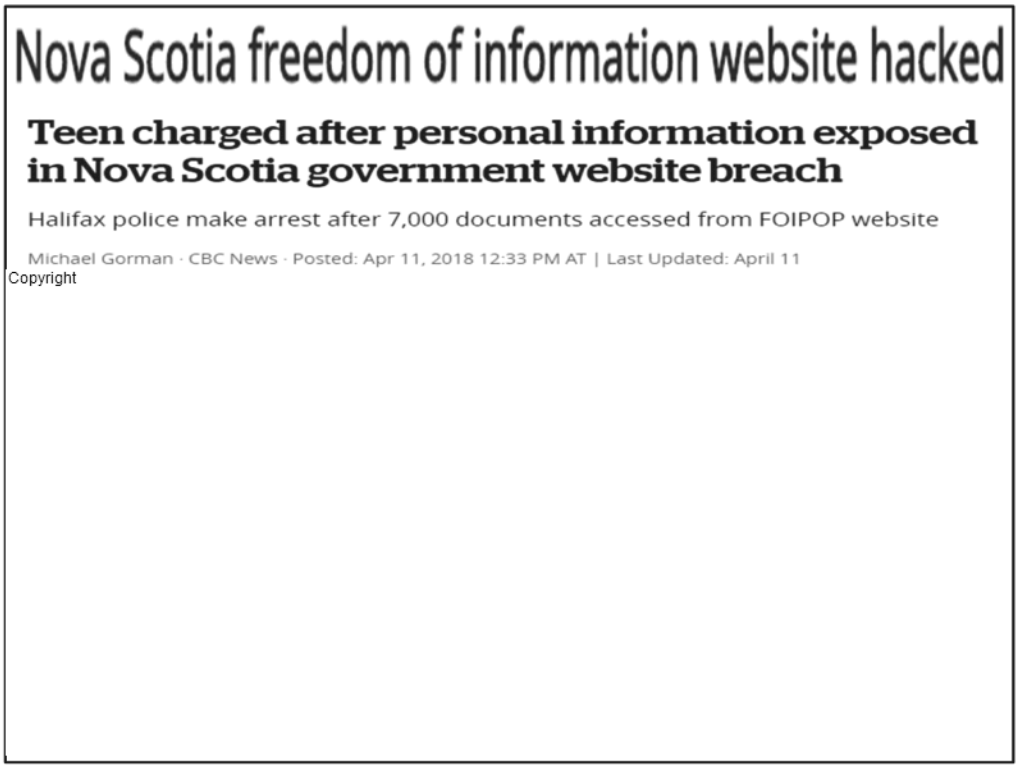
Copyright

How a Typo Stopped Hackers from Stealing $1 Billion from Bank

Friday, March 11, 2016 Swati Khandelwal

Copyright

Copyright



Nova Scotia freedom of information website hacked

Teen charged after personal information exposed in Nova Scotia government website breach

Halifax police make arrest after 7,000 documents accessed from FOIPOP website

Michael Gorman · CBC News · Posted: Apr 11, 2018 12:33 PM AT | Last Updated: April 11

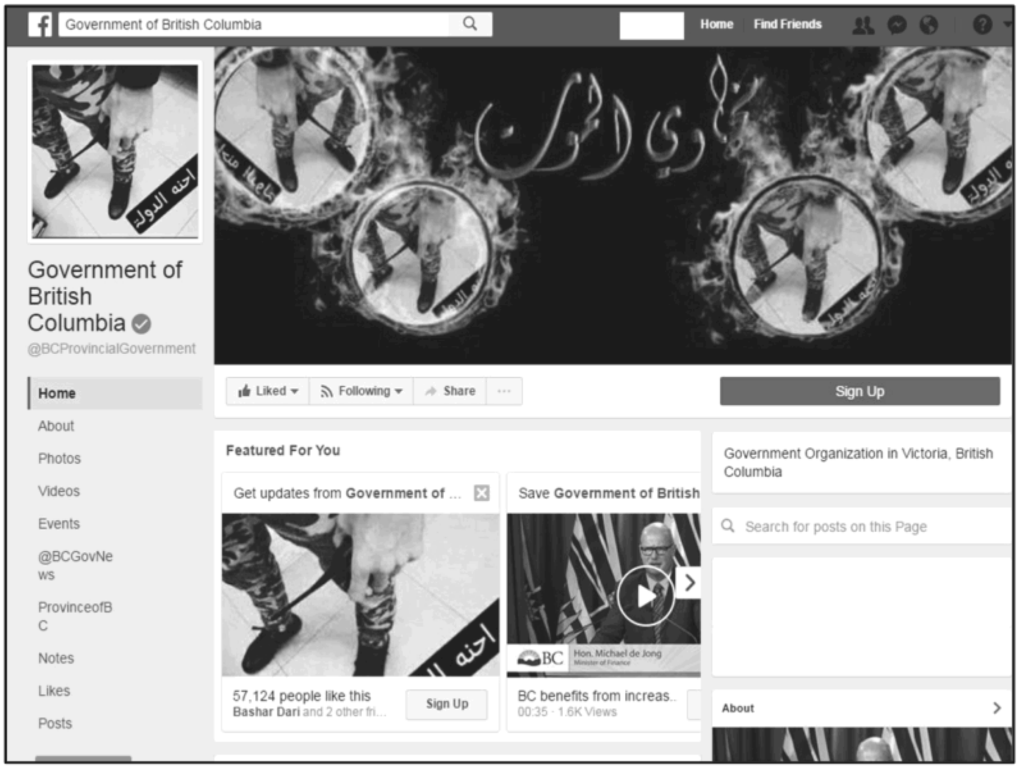
Copyright

P.E.I. government website running again after ransomware attack

P.E.I. government website hit by ransomware attack

Ryan Ross (ryan.ross@theguardian.pe.ca)
Published: 16 hours ago
Updated: 7 hours ago

Copyright



Government of British Columbia
@BCProvincialGovernment

Featured For You

Get updates from **Government of ...**

57,124 people like this
Bashar Dari and 2 other fri...

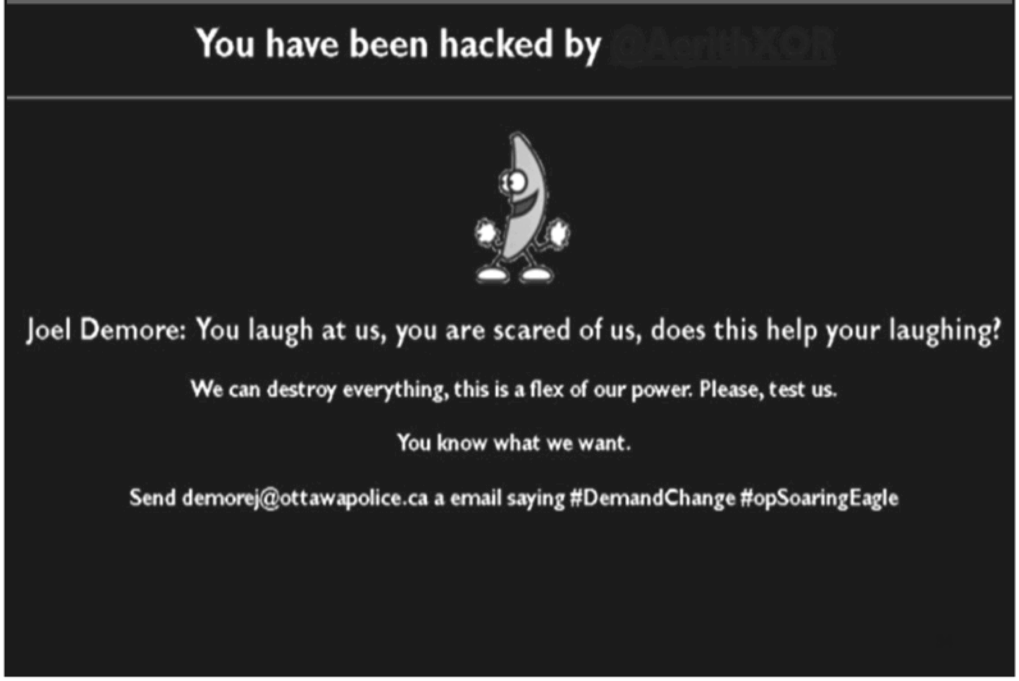
Save **Government of British**

BC benefits from increas..
00:35 · 1.6K Views

Government Organization in Victoria, British Columbia

Gary

Example:



You have been hacked by @AerithXOR

Joel Demore: 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.

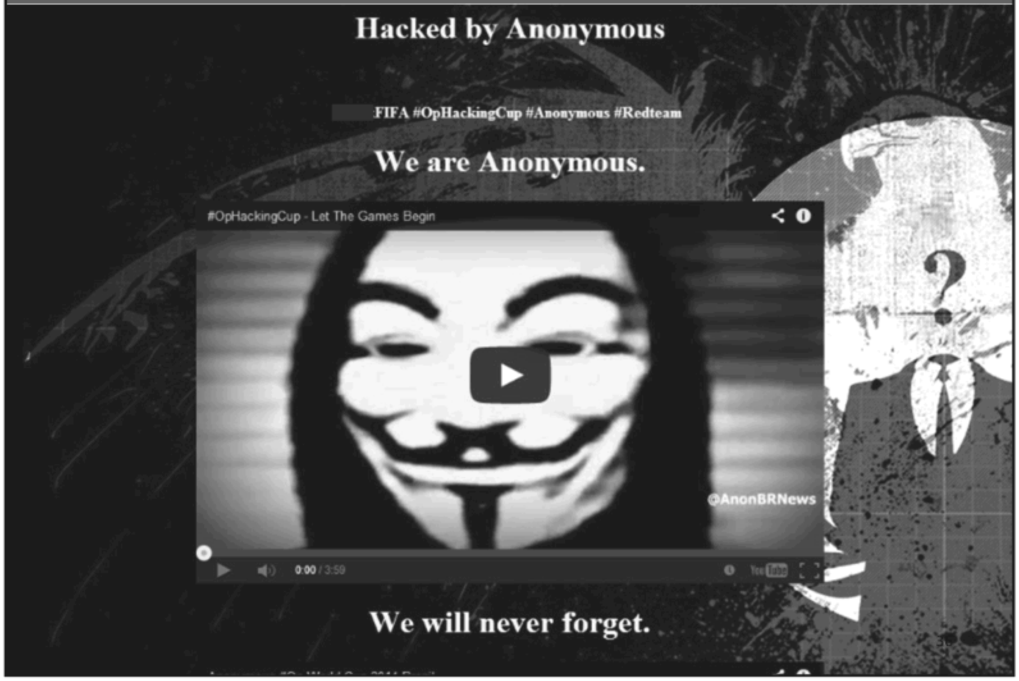
You know what we want.

Send demorej@ottawapolice.ca a email saying #DemandChange #opSoaringEagle

Example:

Copyright

Example:



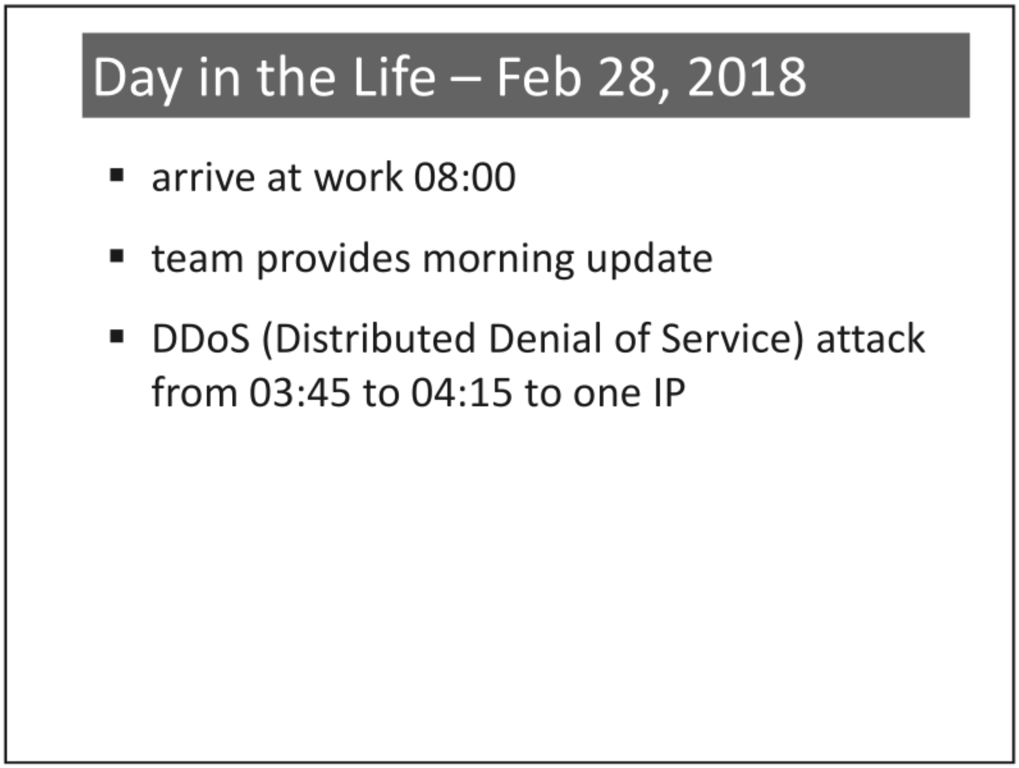
Hacked by Anonymous

FIFA #OpHackingCup #Anonymous #Redteam

We are Anonymous.

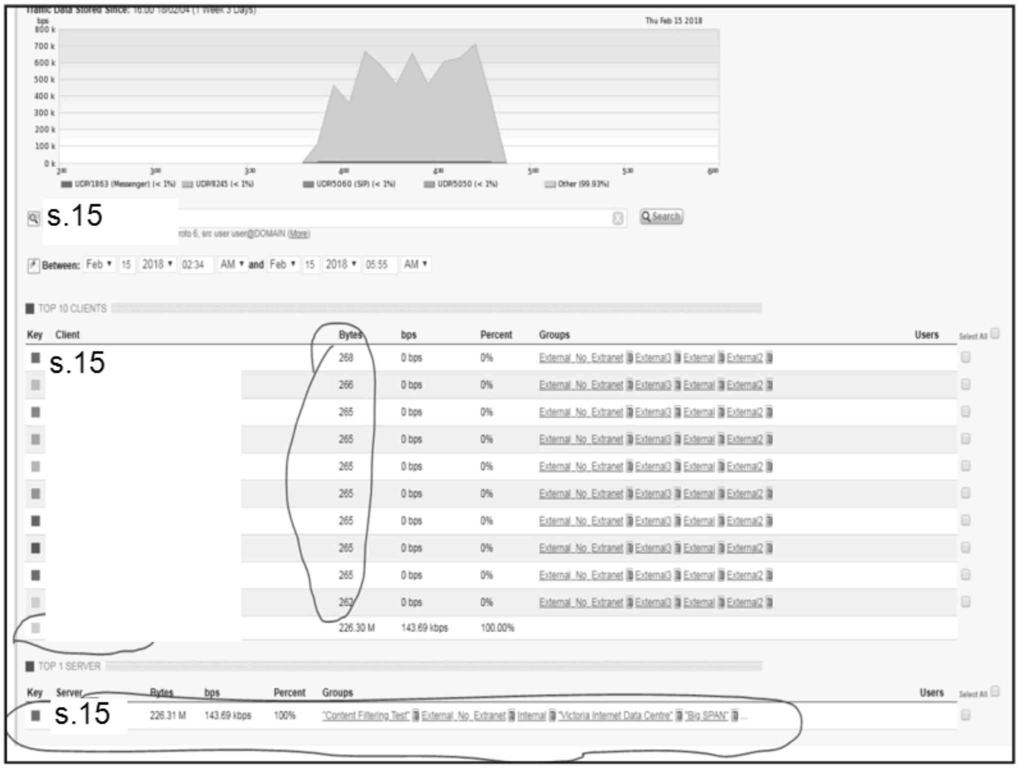
#OpHackingCup - Let The Games Begin

We will never forget.



Day in the Life – Feb 28, 2018

- arrive at work 08:00
- team provides morning update
- DDoS (Distributed Denial of Service) attack from 03:45 to 04:15 to one IP



Traffic Data Stored Since: 16:00 18/02/04 (1 Week 3 Days)

Thu Feb 15 2018

s.15 roto 6, src user user@DOMAIN (More)

Between: Feb ▾ 15 2018 ▾ 02:34 AM ▾ and Feb ▾ 15 2018 ▾ 05:55 AM ▾

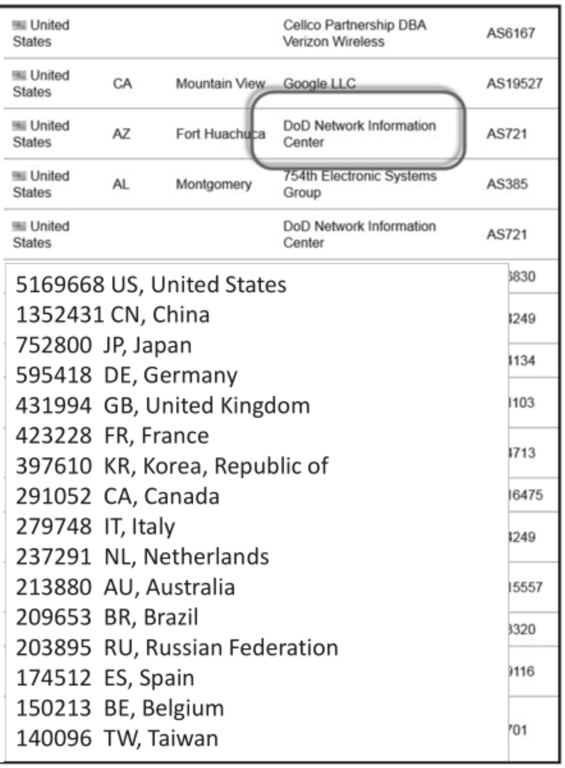
TOP 10 CLIENTS

Key	Client	Bytes	bps	Percent	Groups	Users	Select All □
■	s.15	268	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		266	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		265	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		262	0 bps	0%	External_No_Extranet ▮ External3 ▮ External ▮ External2 ▮		□
■		226.30 M	143.69 kbps	100.00%			

TOP 1 SERVER

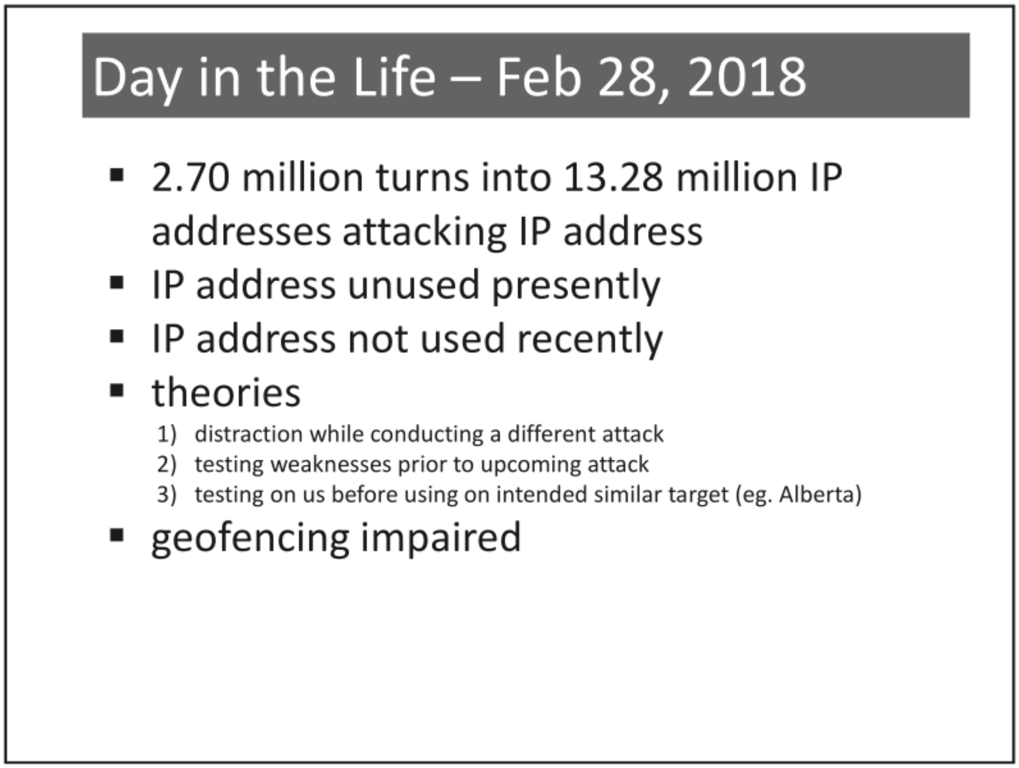
Key	Server	Bytes	bps	Percent	Groups	Users	Select All □
■	s.15	226.31 M	143.69 kbps	100%	"Content Filtering Test" ▮ External_No_Extranet ▮ Internal ▮ "Victoria Internet Data Centre" ▮ "Big SPAN" ▮ ...		□

s.15



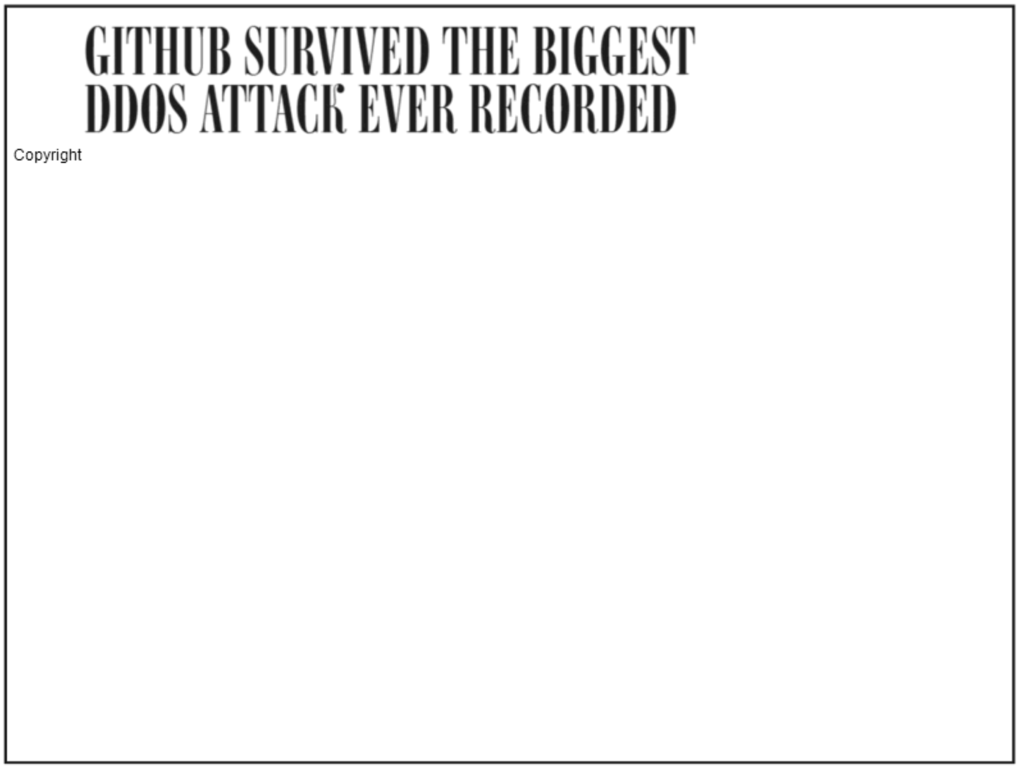
United States			Cellco Partnership DBA Verizon Wireless	AS6167
United States	CA	Mountain View	Google LLC	AS19527
United States	AZ	Fort Huachuca	DoD Network Information Center	AS721
United States	AL	Montgomery	754th Electronic Systems Group	AS385
United States			DoD Network Information Center	AS721
				830
				249
				134
				103
				713
				6475
				249
				5557
				320
				116
				01

5169668	US, United States
1352431	CN, China
752800	JP, Japan
595418	DE, Germany
431994	GB, United Kingdom
423228	FR, France
397610	KR, Korea, Republic of
291052	CA, Canada
279748	IT, Italy
237291	NL, Netherlands
213880	AU, Australia
209653	BR, Brazil
203895	RU, Russian Federation
174512	ES, Spain
150213	BE, Belgium
140096	TW, Taiwan



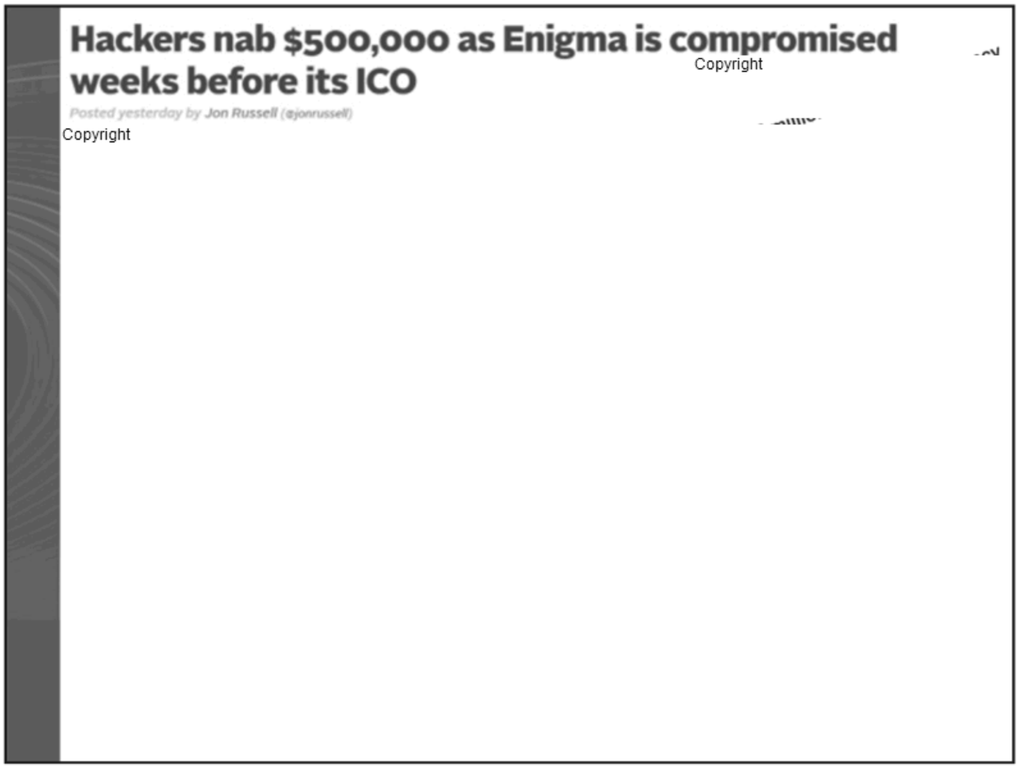
Day in the Life – Feb 28, 2018

- 2.70 million turns into 13.28 million IP addresses attacking IP address
- IP address unused presently
- IP address not used recently
- theories
  1) distraction while conducting a different attack
  2) testing weaknesses prior to upcoming attack
  3) testing on us before using on intended similar target (eg. Alberta)
- geofencing impaired



GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

Copyright



Hackers nab $500,000 as Enigma is compromised weeks before its ICO

Posted yesterday by Jon Russell (@jonrussell)

Copyright

Copyright

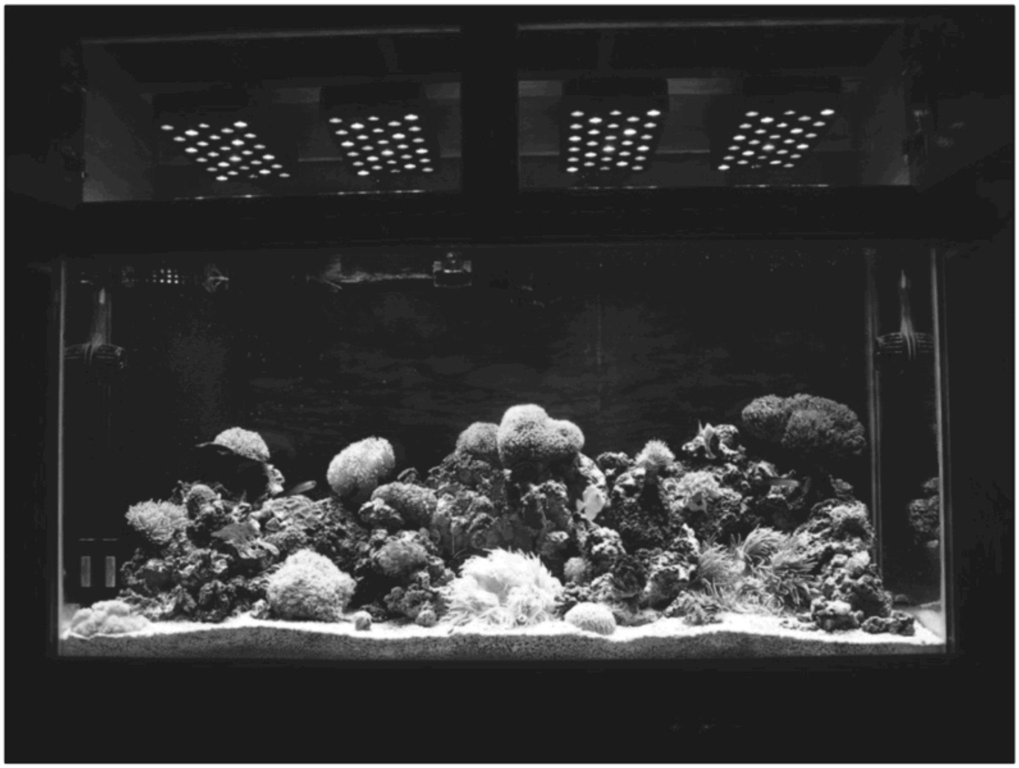
Copyright

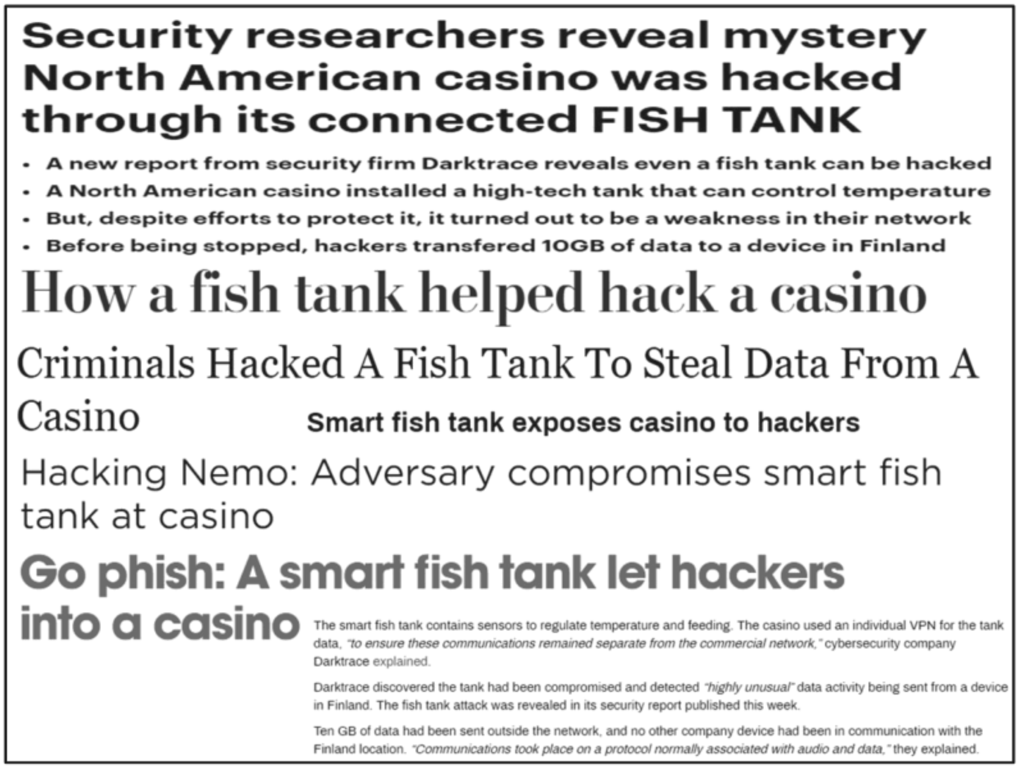
Ashley Madison hack victims receive blackmail letters

Page 44

Withheld pursuant to/removed as

s.15





Security researchers reveal mystery North American casino was hacked through its connected FISH TANK

- A new report from security firm Darktrace reveals even a fish tank can be hacked
- A North American casino installed a high-tech tank that can control temperature
- But, despite efforts to protect it, it turned out to be a weakness in their network
- Before being stopped, hackers transfered 10GB of data to a device in Finland

How a fish tank helped hack a casino

Criminals Hacked A Fish Tank To Steal Data From A Casino

Smart fish tank exposes casino to hackers

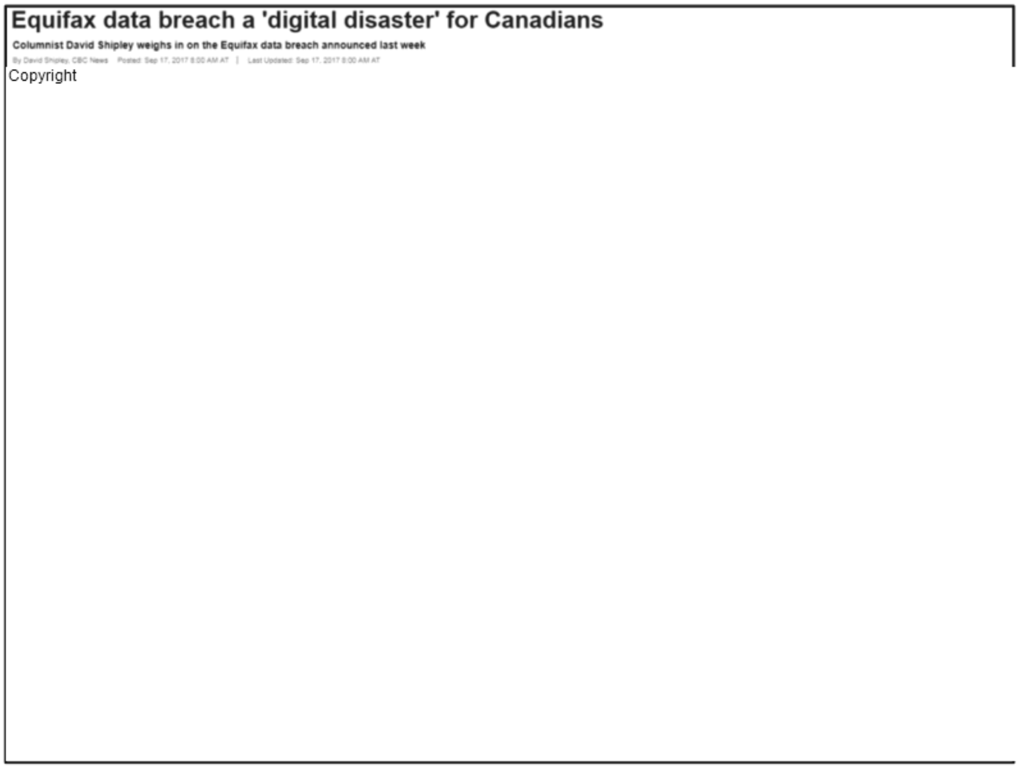
Hacking Nemo: Adversary compromises smart fish tank at casino

Go phish: A smart fish tank let hackers into a casino

The smart fish tank contains sensors to regulate temperature and feeding. The casino used an individual VPN for the tank data, *"to ensure these communications remained separate from the commercial network,"* cybersecurity company Darktrace explained.

Darktrace discovered the tank had been compromised and detected *"highly unusual"* data activity being sent from a device in Finland. The fish tank attack was revealed in its security report published this week.

Ten GB of data had been sent outside the network, and no other company device had been in communication with the Finland location. *"Communications took place on a protocol normally associated with audio and data,"* they explained.



Equifax data breach a 'digital disaster' for Canadians

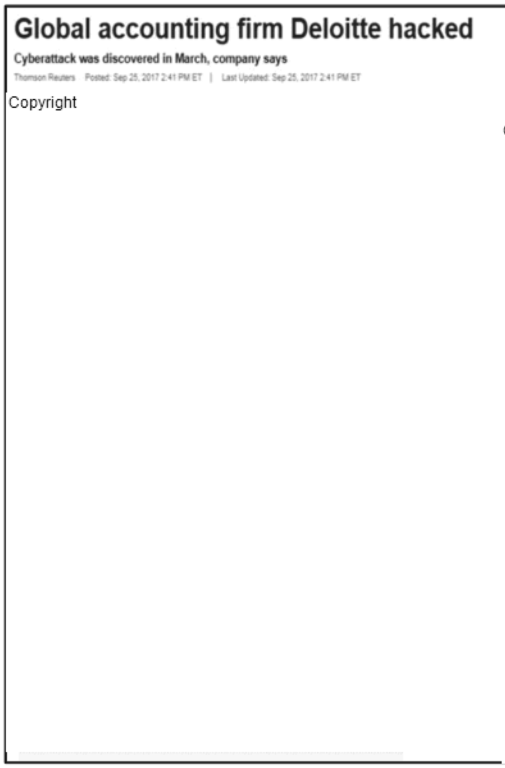
Columnist David Shipley weighs in on the Equifax data breach announced last week

By David Shipley, CBC News   Posted: Sep 17, 2017 8:00 AM AT | Last Updated: Sep 17, 2017 8:00 AM AT

Copyright

Equifax CEO out amid fallout from data breach

Copyright

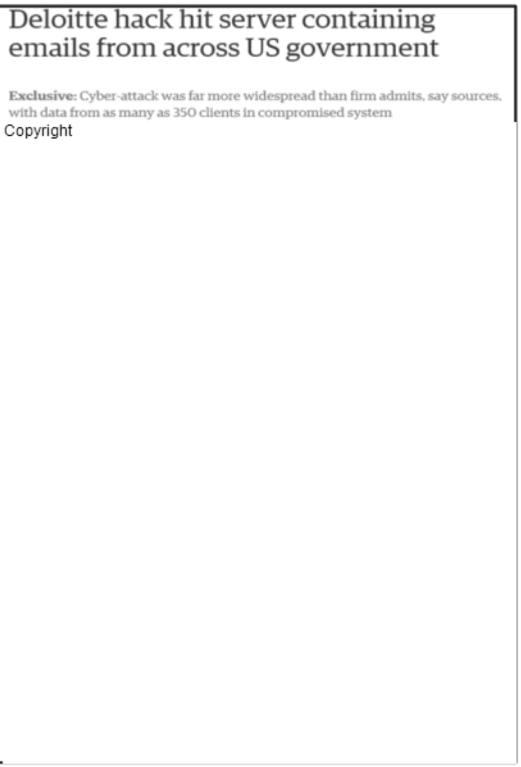


Global accounting firm Deloitte hacked

Cyberattack was discovered in March, company says

Thomson Reuters · Posted: Sep 25, 2017 2:41 PM ET | Last Updated: Sep 25, 2017 2:41 PM ET

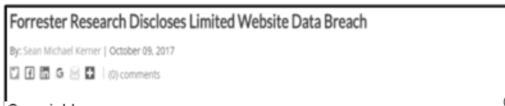
Copyright



Deloitte hack hit server containing emails from across US government

Exclusive: Cyber-attack was far more widespread than firm admits, say sources, with data from as many as 350 clients in compromised system

Copyright

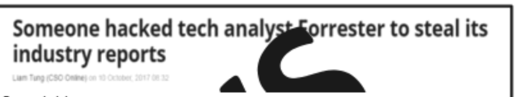


Forrester Research Discloses Limited Website Data Breach

By: Sean Michael Kerner | October 09, 2017

(0) comments

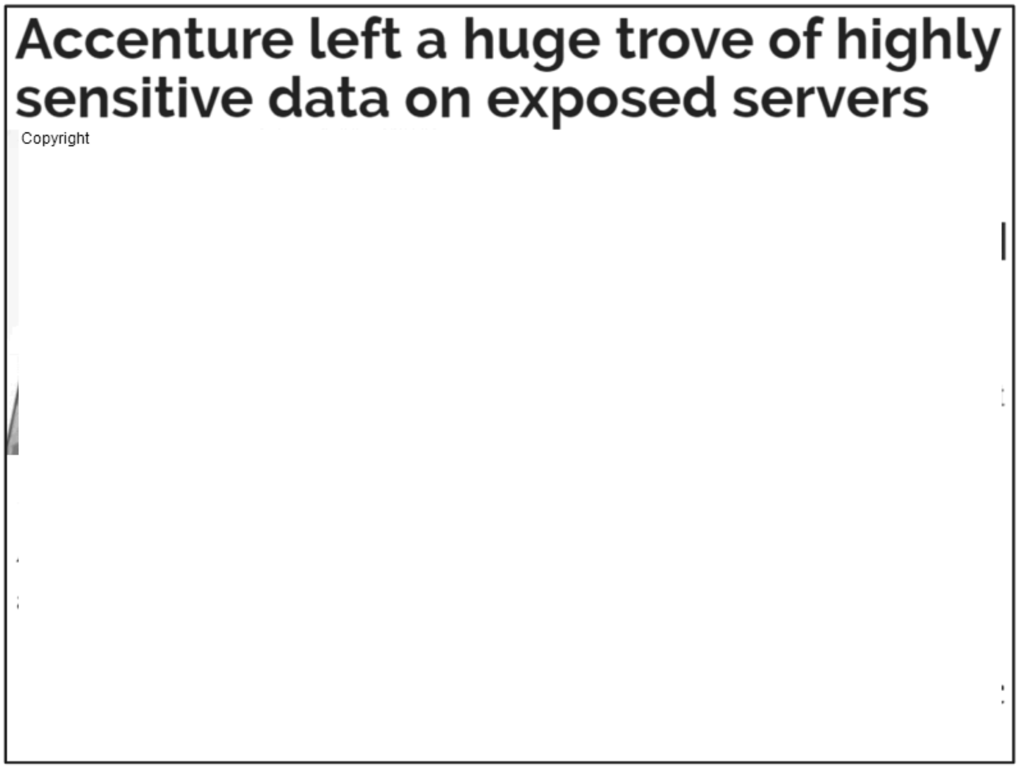
Copyright



Someone hacked tech analyst Forrester to steal its industry reports

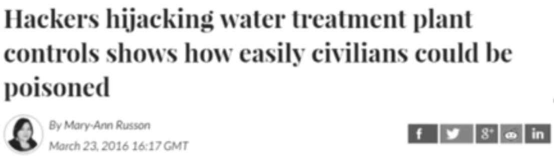
Liam Tung (CSO Online) on 10 October, 2017 08:32

Copyright



Accenture left a huge trove of highly sensitive data on exposed servers

Copyright



Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned

By Mary-Ann Russon
March 23, 2016 16:17 GMT

Copyright

Hackers Breach Water Treatment Plant, Alter Chemicals in Water Supply

The hackers 'modified application settings with little apparent knowledge of how the flow control system worked,' according to a Verizon report.

By Jeff Goldman | Posted March 28, 2016

Copyright

Cyberattack that crippled Ukrainian power grid was highly coordinated

1st power outage caused by cyberattack suggests similar attacks possible around the globe

Thomson Reuters Posted: Jan 11, 2016 11:52 AM ET | Last Updated: Jan 11, 2016 12:17 PM ET

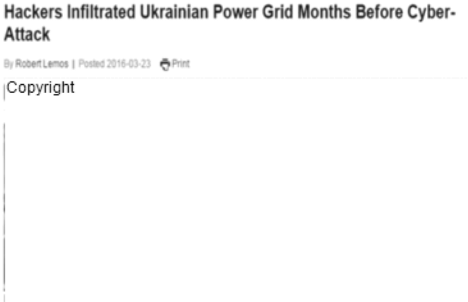
Copyright

Hackers did indeed cause Ukrainian power outage, US report concludes

DHS officials say well-coordinated hack cut power to 225,000 people.

by Dan Goodin - Feb 26, 2016 11:14am PST

Copyright



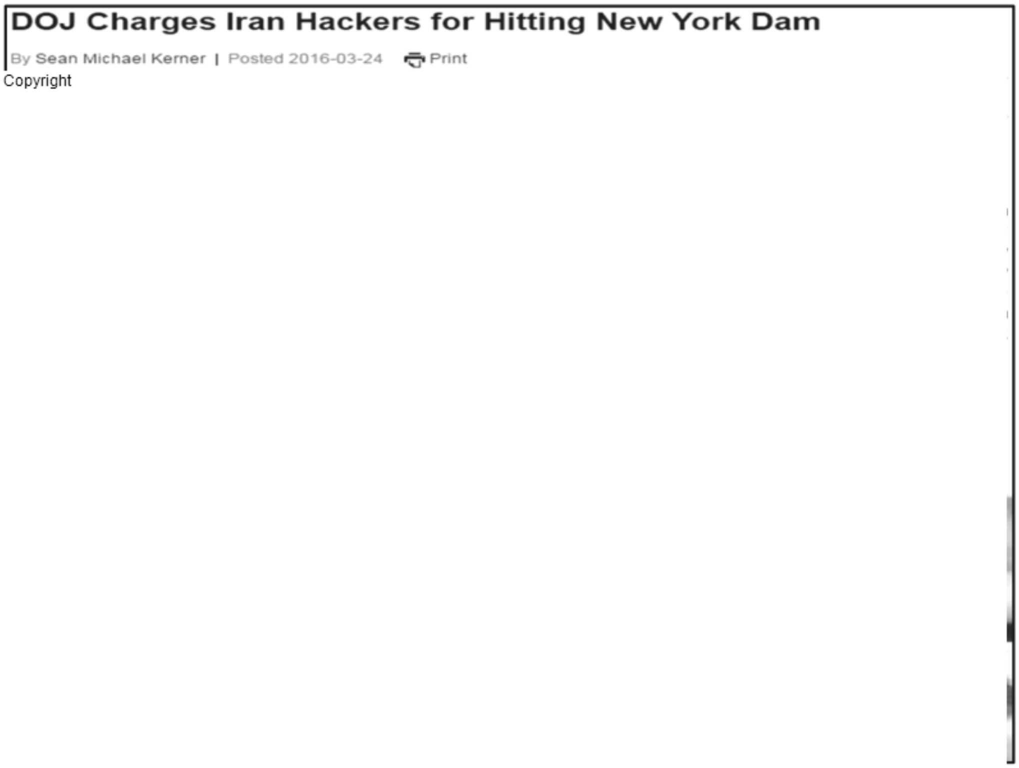
Hackers Infiltrated Ukrainian Power Grid Months Before Cyber-Attack

By Robert Lemos | Posted 2016-03-23 Print

Copyright

DHS: CYBERATTACK ON THE UKRAINE POWER GRID COULD HAPPEN HERE

Copyright

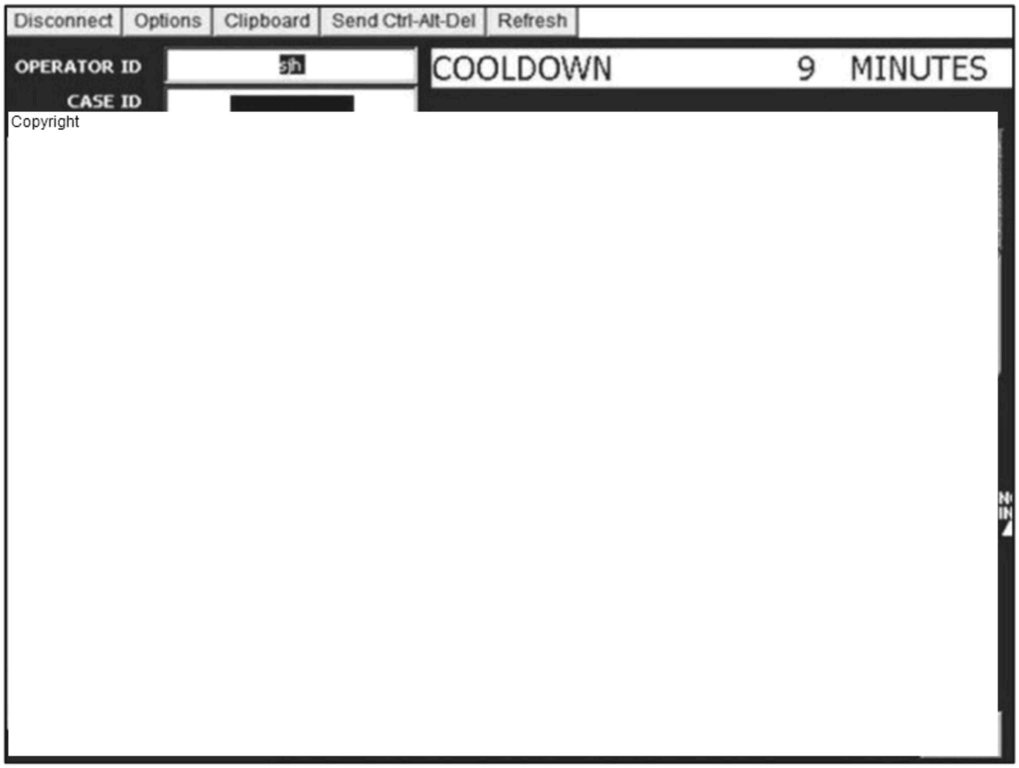


DOJ Charges Iran Hackers for Hitting New York Dam

By Sean Michael Kerner | Posted 2016-03-24 Print

Copyright

Raw Water
Bass Ridge
Cardinal Park
Richerson
Industrial Park
Spurlington
Elkhorn
Speck
Chlorine Monitor
Reload Main
Copyright



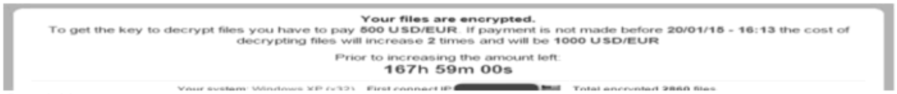
OPERATOR ID sjh

CASE ID [redacted]

COOLDOWN 9 MINUTES

Copyright

Ransomware Example



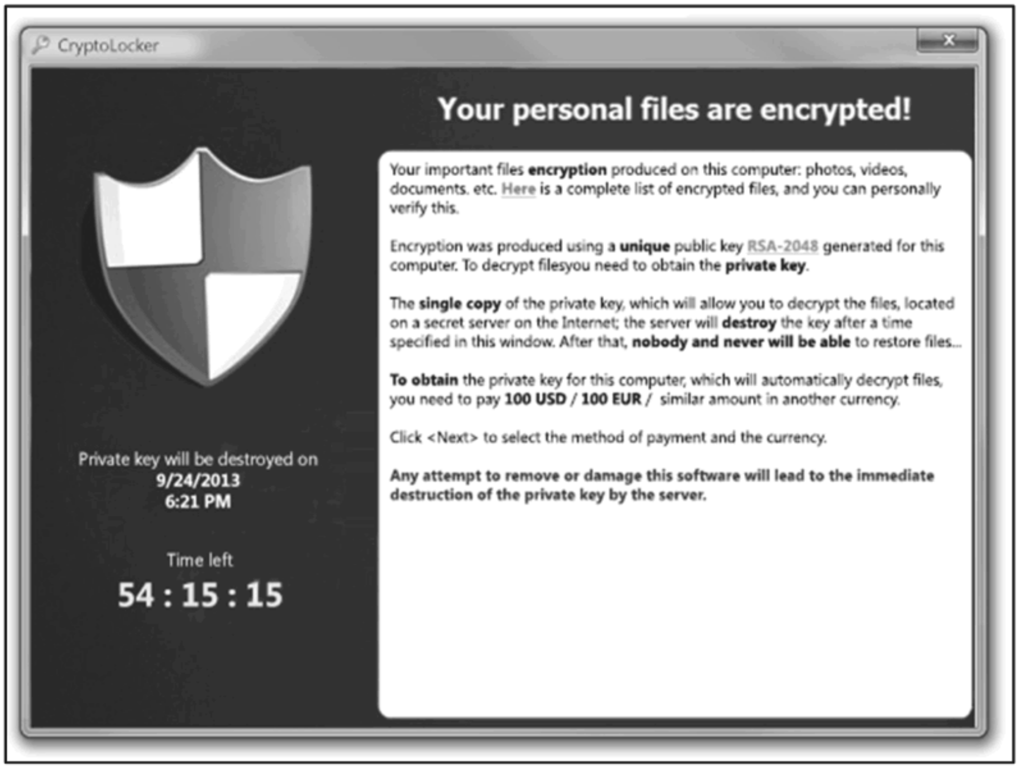
Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h 59m 00s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted **2860** files

Copyright

Anyone hit by Cryptolocker?



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

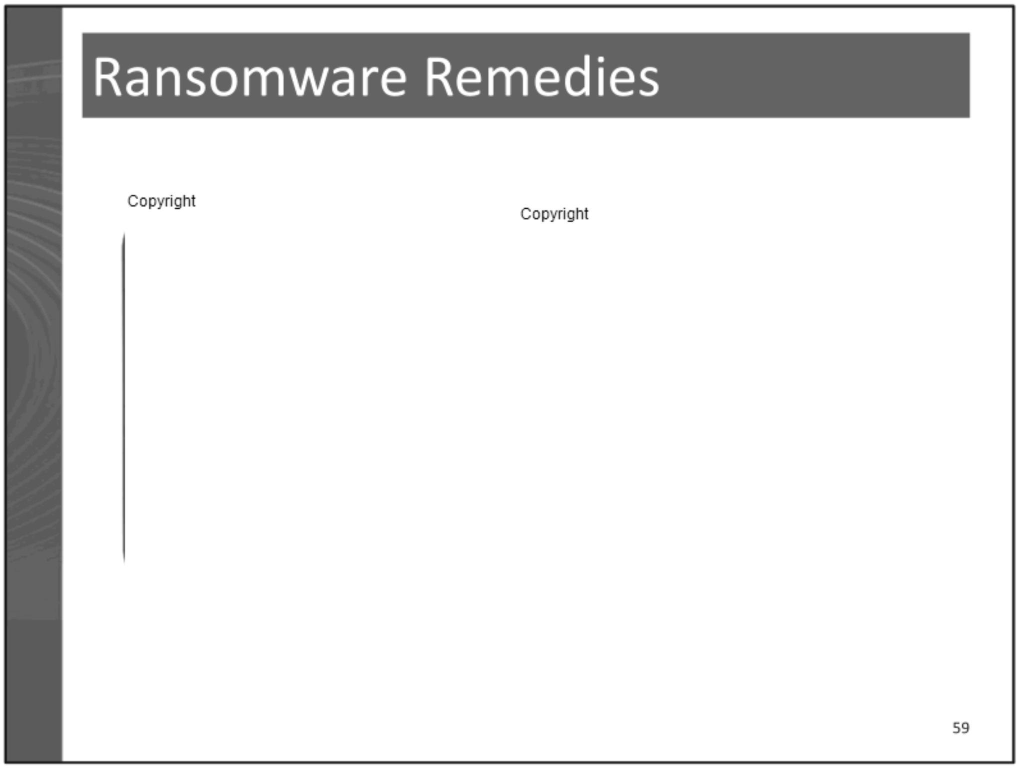
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

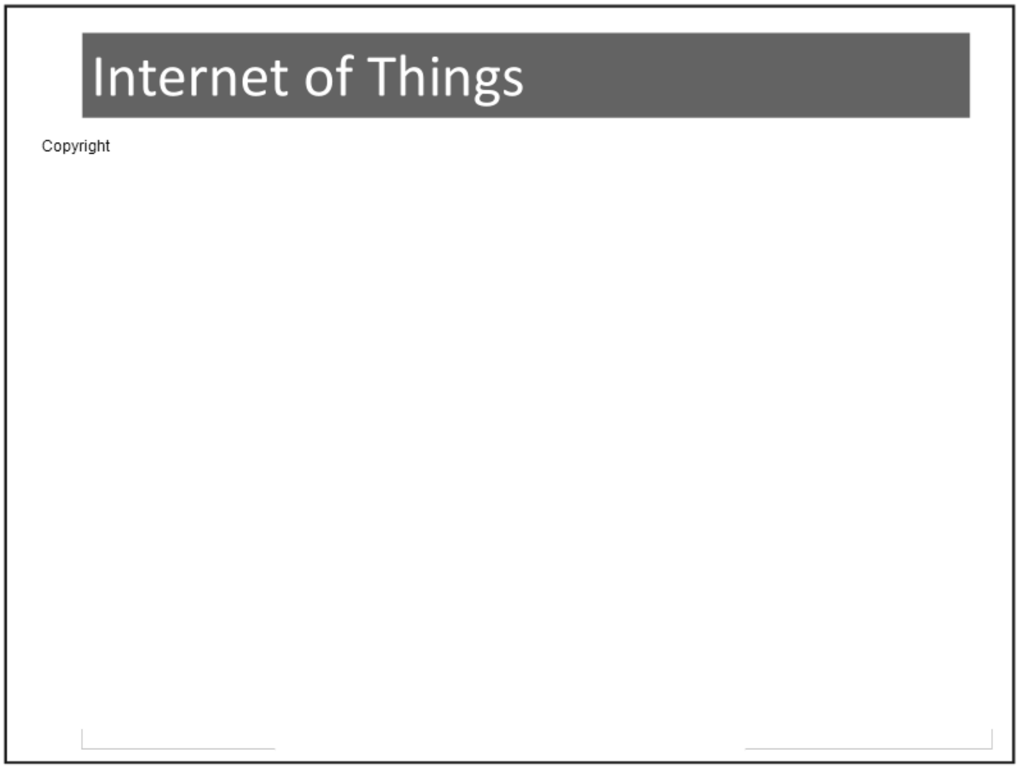
Time left
54 : 15 : 15



Ransomware Remedies

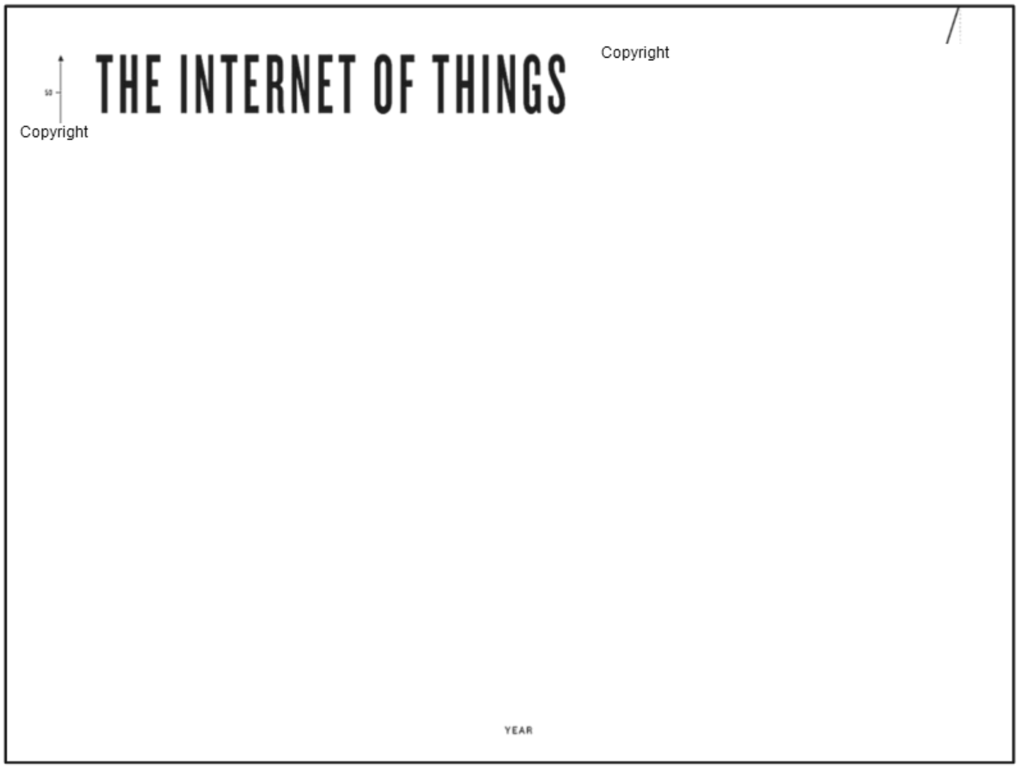
Copyright

Copyright



Internet of Things

Copyright

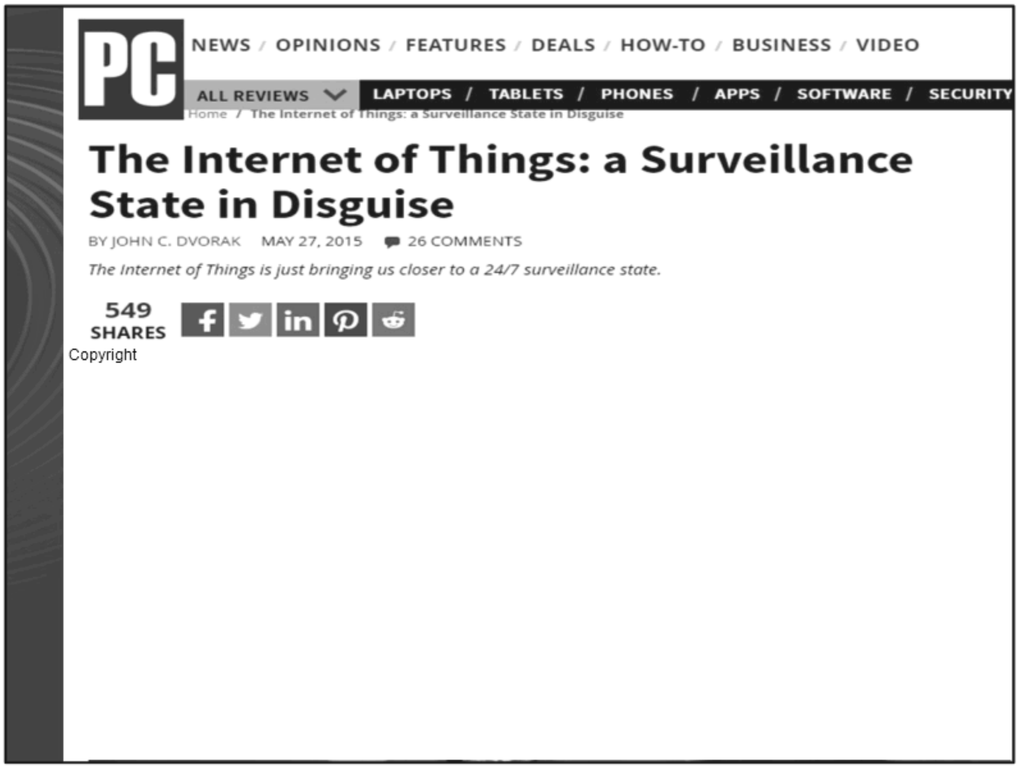


- aka Internet of Everything
- aka Internet of Threats
- aka Internet of Vulnerabilities

Copyright

Copyright

Copyright

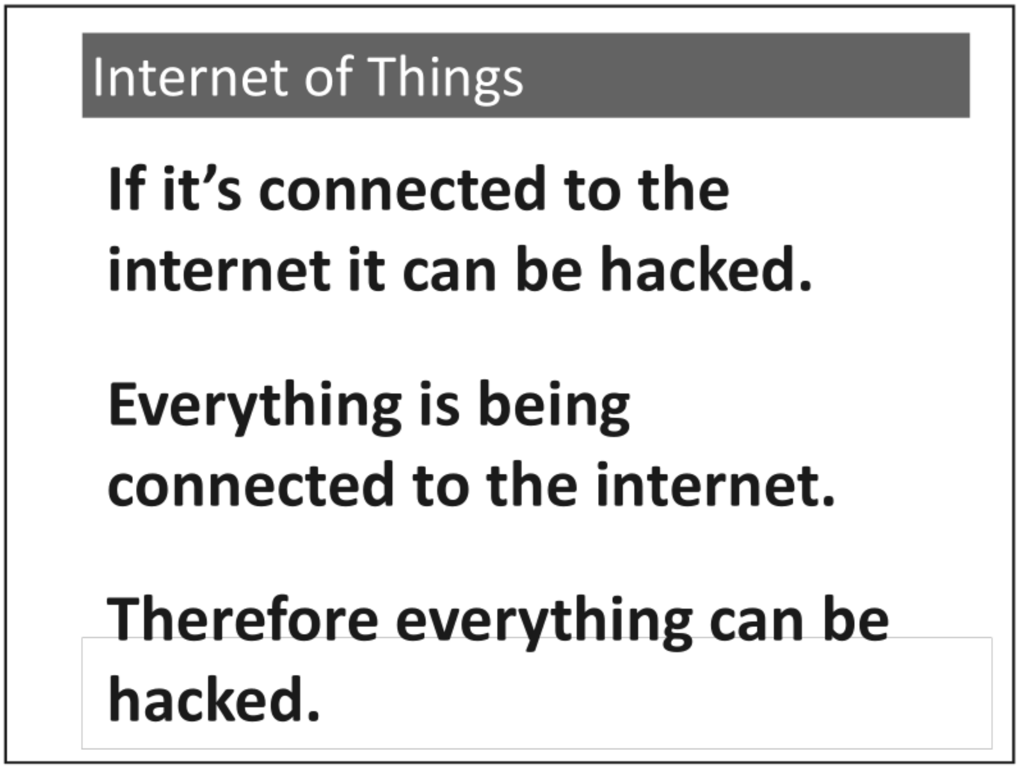

PC
NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / VIDEO
ALL REVIEWS
LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY
Home / The Internet of Things: a Surveillance State in Disguise

The Internet of Things: a Surveillance State in Disguise

BY JOHN C. DVORAK MAY 27, 2015 26 COMMENTS

The Internet of Things is just bringing us closer to a 24/7 surveillance state.

Copyright



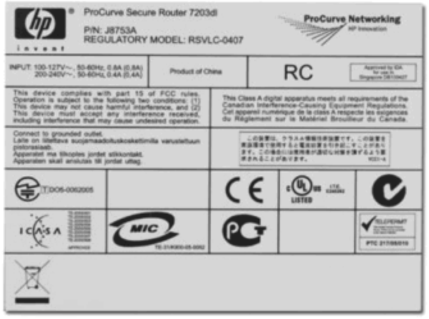
Internet of Things

If it’s connected to the internet it can be hacked.

Everything is being connected to the internet.

Therefore everything can be hacked.

Standards



ProCurve Secure Router 7203dl

P/N: J8753A
REGULATORY MODEL: RSVLC-0407

INPUT: 100-127V~, 50-60Hz, 0.8A (0.8A)
200-240V~, 50-60Hz, 0.4A (0.4A)

Product of China

This device complies with part 15 of FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

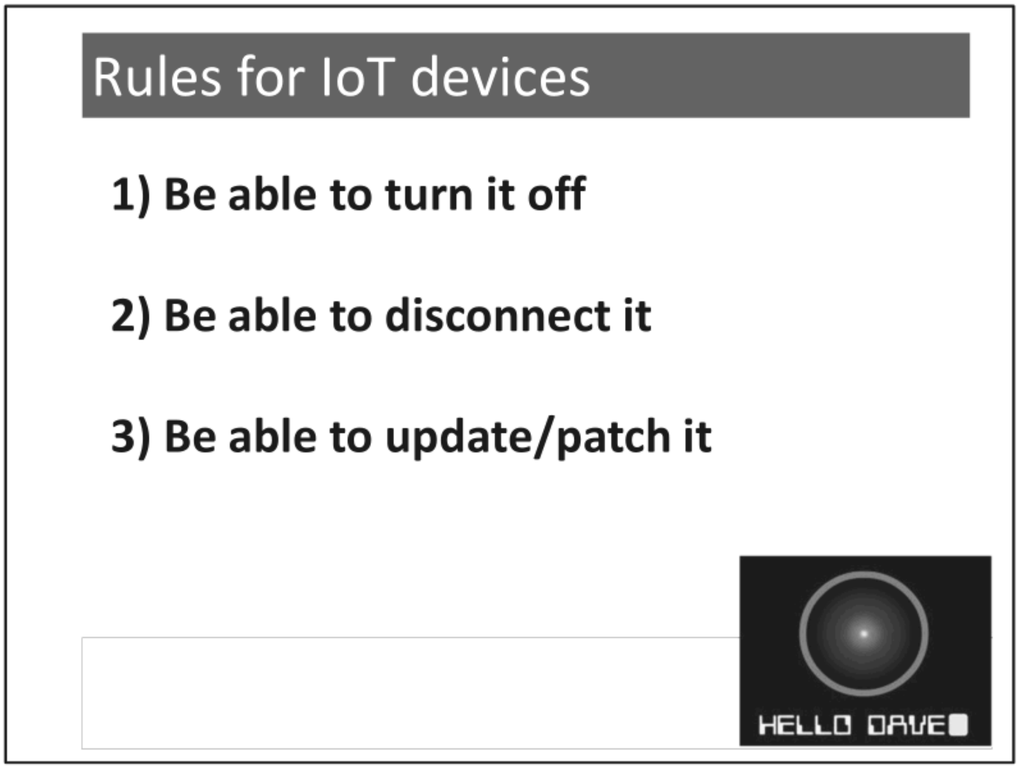
This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la class A respecte les exigences du Règlement sur le Matériel Brouilleur du Canada.

Connect to grounded outlet.
Laite on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan.
Apparatet ma tilkoples jordet stikkontakt.
Apparaten skall anslutas till jordat uttag.

[illegible]

T D05-0062005

PTC 217/06/010



Rules for IoT devices

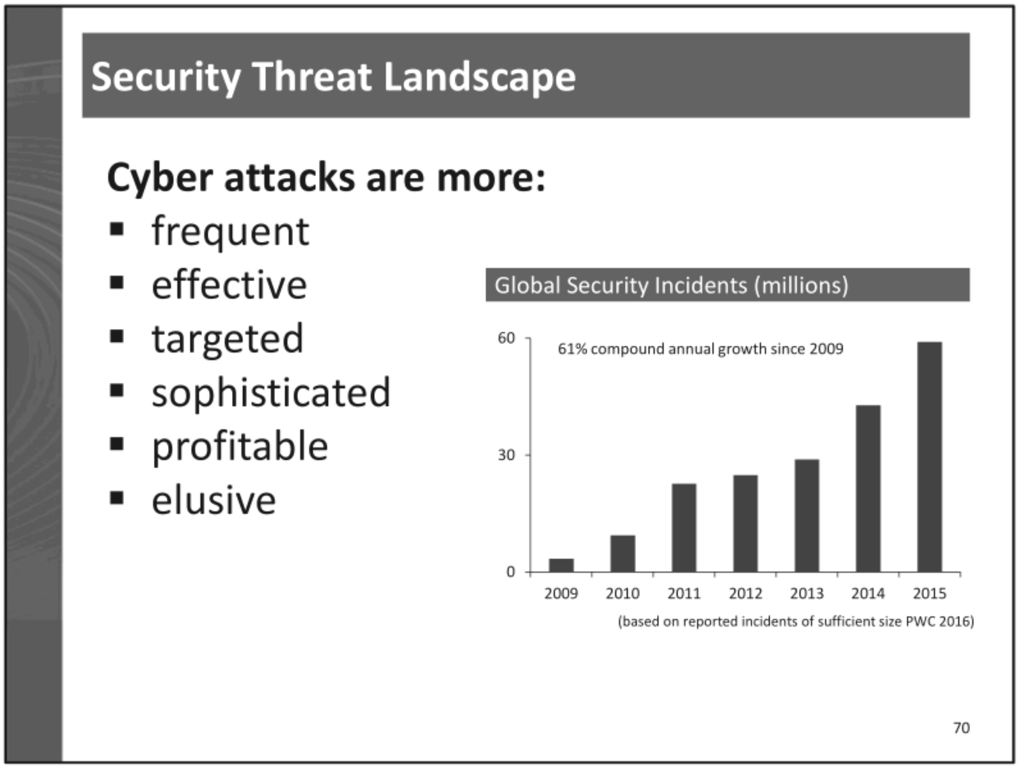
1) Be able to turn it off

2) Be able to disconnect it

3) Be able to update/patch it

Threats to Critical Infrastructure

Copyright



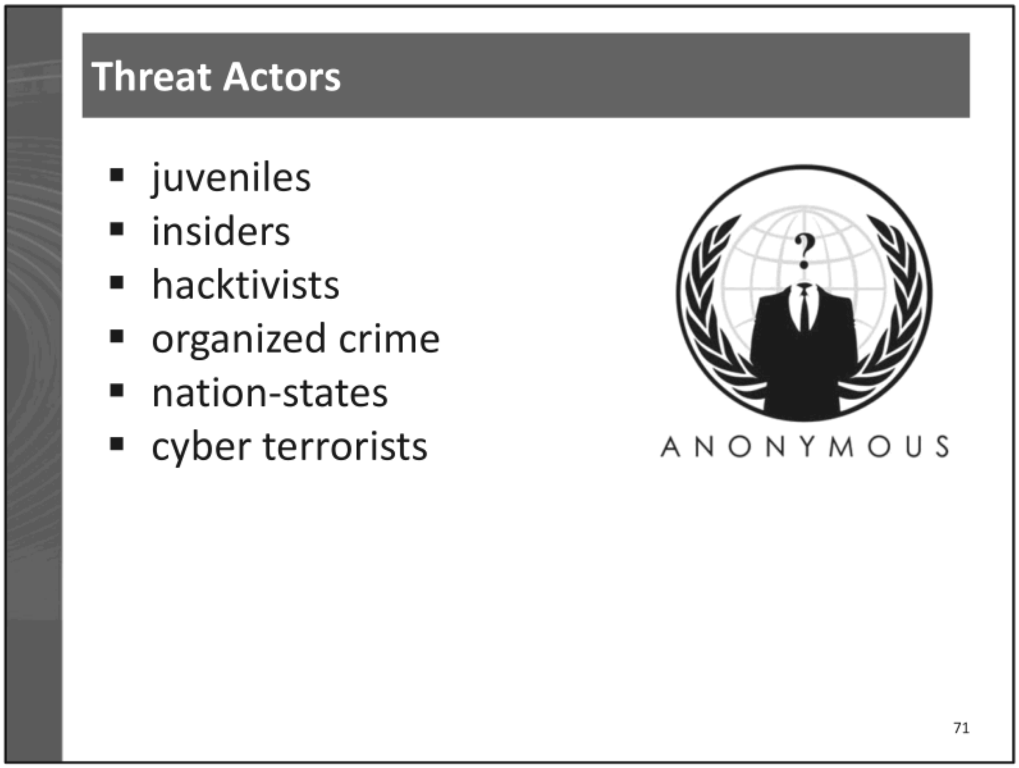
Security Threat Landscape

Cyber attacks are more:

- frequent
- effective
- targeted
- sophisticated
- profitable
- elusive

Global Security Incidents (millions)

(based on reported incidents of sufficient size PWC 2016)



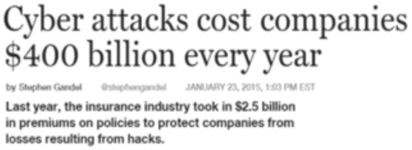
Threat Actors

- juveniles
- insiders
- hacktivists
- organized crime
- nation-states
- cyber terrorists

Business Impacts

- direct impact to clients
- financial, value loss
- litigation, regulatory
- data breach and loss
- brand and reputation
- lost/stolen intellectual property
- lost productivity

In the news



Cyber attacks cost companies $400 billion every year

by Stephen Gandel @stephengandel JANUARY 23, 2015, 1:03 PM EST

Last year, the insurance industry took in $2.5 billion in premiums on policies to protect companies from losses resulting from hacks.

Why Organizations are Targeted

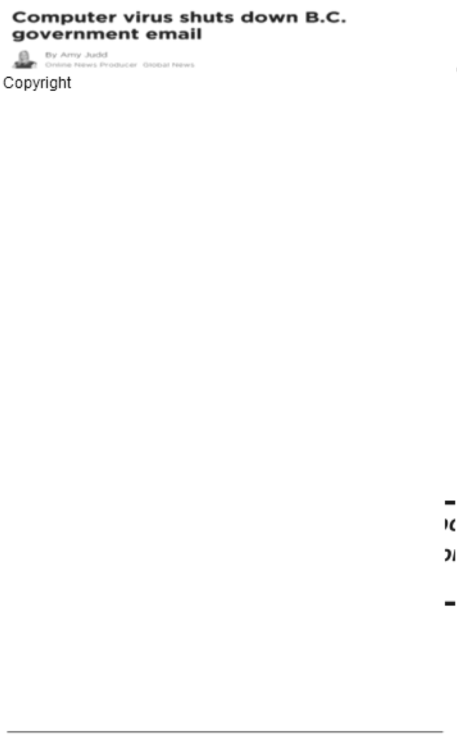
- gain economic advantage
- access to personal data (ie. health), fraud
- trusted launch point against others
- law enforcement, justice, court services
- surveillance

In the news

Personal info of 15,000 people accessed in B.C. government database breach

Government traditional security controls block millions of attacks daily

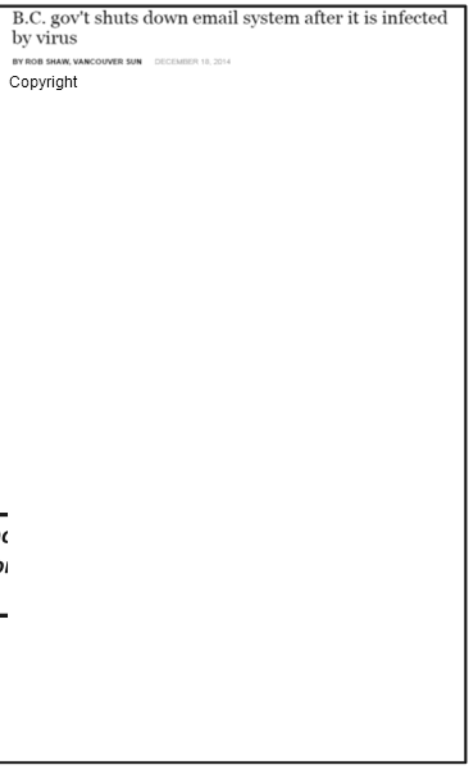
Copyright



Computer virus shuts down B.C. government email

By Amy Judd
Online News Producer Global News

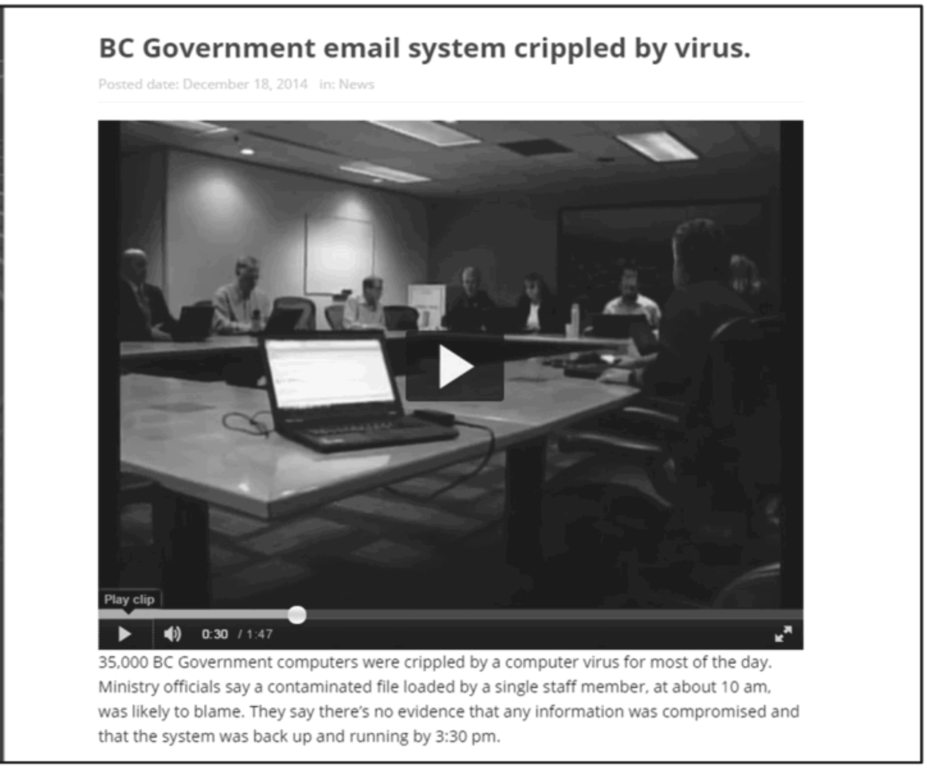
Copyright



B.C. gov't shuts down email system after it is infected by virus

BY ROB SHAW, VANCOUVER SUN DECEMBER 18, 2014

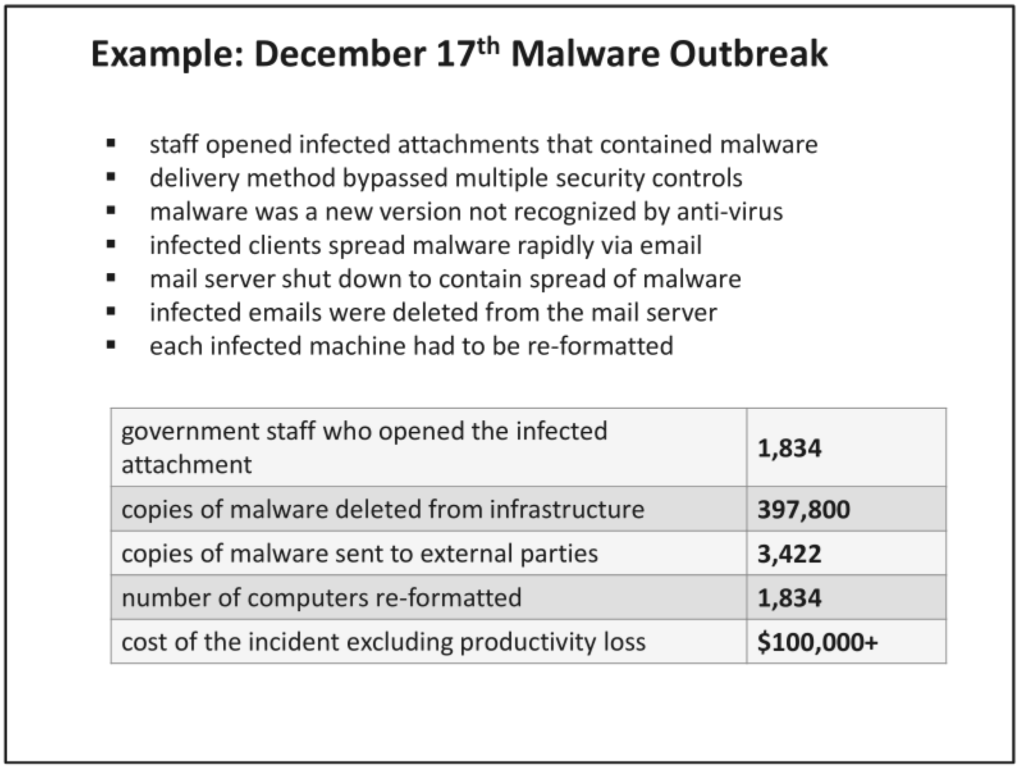
Copyright



BC Government email system crippled by virus.

Posted date: December 18, 2014 in: News

35,000 BC Government computers were crippled by a computer virus for most of the day. Ministry officials say a contaminated file loaded by a single staff member, at about 10 am, was likely to blame. They say there's no evidence that any information was compromised and that the system was back up and running by 3:30 pm.



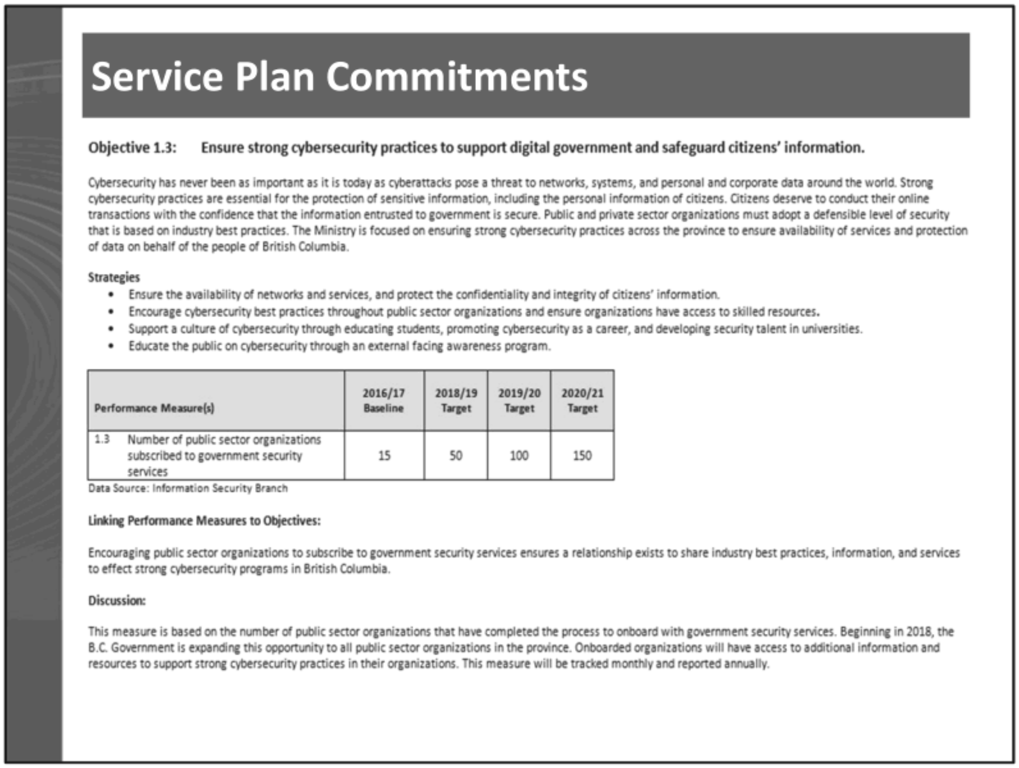
Example: December 17th Malware Outbreak

- staff opened infected attachments that contained malware
- delivery method bypassed multiple security controls
- malware was a new version not recognized by anti-virus
- infected clients spread malware rapidly via email
- mail server shut down to contain spread of malware
- infected emails were deleted from the mail server
- each infected machine had to be re-formatted

government staff who opened the infected attachment	**1,834**
copies of malware deleted from infrastructure	**397,800**
copies of malware sent to external parties	**3,422**
number of computers re-formatted	**1,834**
cost of the incident excluding productivity loss	**$100,000+**

Government’s response to the evolving threat landscape

Copyright



Service Plan Commitments

Objective 1.3: Ensure strong cybersecurity practices to support digital government and safeguard citizens' information.

Cybersecurity has never been as important as it is today as cyberattacks pose a threat to networks, systems, and personal and corporate data around the world. Strong cybersecurity practices are essential for the protection of sensitive information, including the personal information of citizens. Citizens deserve to conduct their online transactions with the confidence that the information entrusted to government is secure. Public and private sector organizations must adopt a defensible level of security that is based on industry best practices. The Ministry is focused on ensuring strong cybersecurity practices across the province to ensure availability of services and protection of data on behalf of the people of British Columbia.

Strategies

- Ensure the availability of networks and services, and protect the confidentiality and integrity of citizens' information.
- Encourage cybersecurity best practices throughout public sector organizations and ensure organizations have access to skilled resources.
- Support a culture of cybersecurity through educating students, promoting cybersecurity as a career, and developing security talent in universities.
- Educate the public on cybersecurity through an external facing awareness program.

Performance Measure(s)	2016/17 Baseline	2018/19 Target	2019/20 Target	2020/21 Target
1.3 Number of public sector organizations subscribed to government security services	15	50	100	150

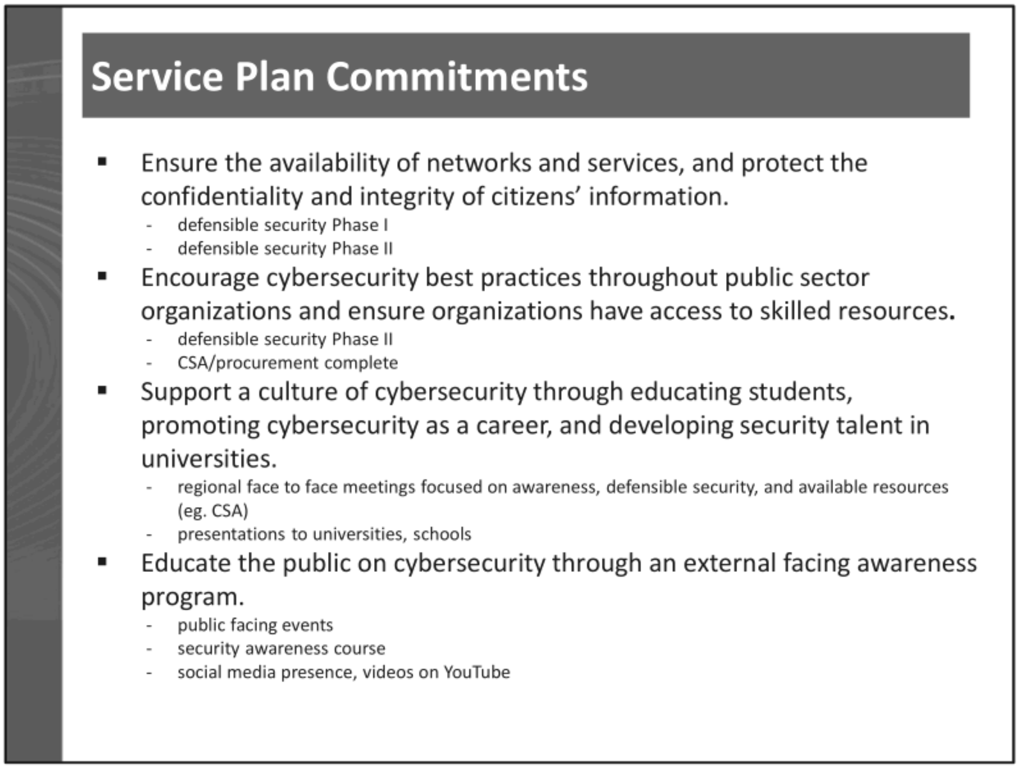
Data Source: Information Security Branch

Linking Performance Measures to Objectives:

Encouraging public sector organizations to subscribe to government security services ensures a relationship exists to share industry best practices, information, and services to effect strong cybersecurity programs in British Columbia.

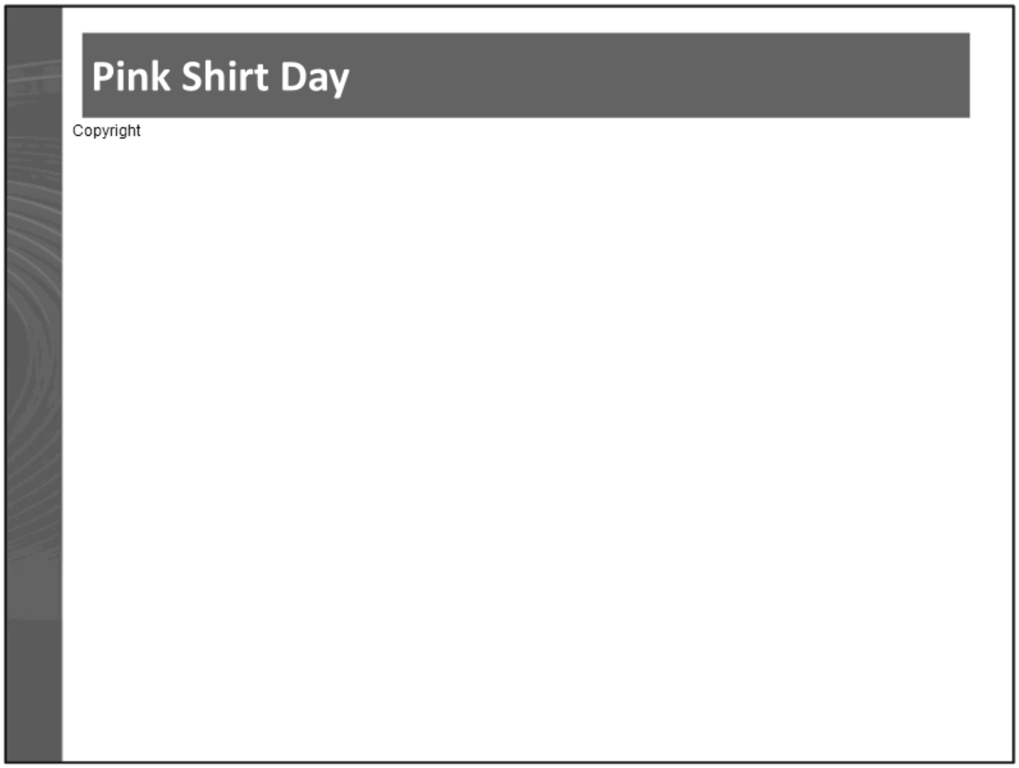
Discussion:

This measure is based on the number of public sector organizations that have completed the process to onboard with government security services. Beginning in 2018, the B.C. Government is expanding this opportunity to all public sector organizations in the province. Onboarded organizations will have access to additional information and resources to support strong cybersecurity practices in their organizations. This measure will be tracked monthly and reported annually.



Service Plan Commitments

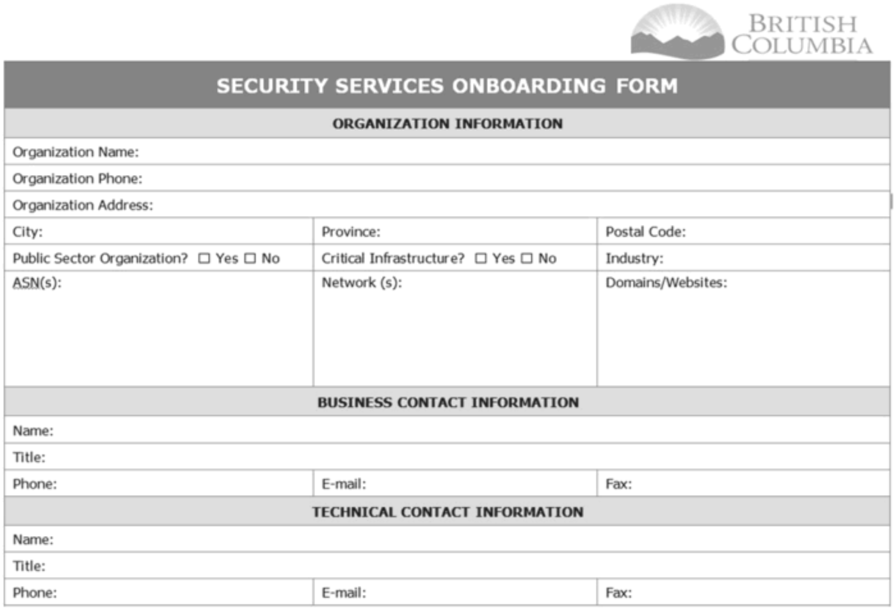
- Ensure the availability of networks and services, and protect the confidentiality and integrity of citizens' information.
  - defensible security Phase I
  - defensible security Phase II
- Encourage cybersecurity best practices throughout public sector organizations and ensure organizations have access to skilled resources**.**
  - defensible security Phase II
  - CSA/procurement complete
- Support a culture of cybersecurity through educating students, promoting cybersecurity as a career, and developing security talent in universities.
  - regional face to face meetings focused on awareness, defensible security, and available resources (eg. CSA)
  - presentations to universities, schools
- Educate the public on cybersecurity through an external facing awareness program.
  - public facing events
  - security awareness course
  - social media presence, videos on YouTube



Pink Shirt Day

Copyright

External Security Services

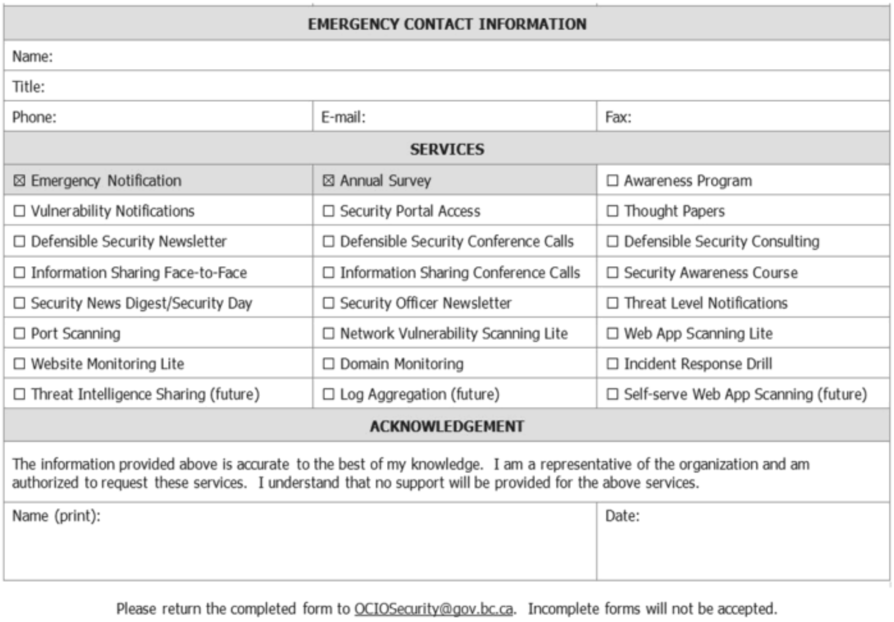


BRITISH COLUMBIA

SECURITY SERVICES ONBOARDING FORM

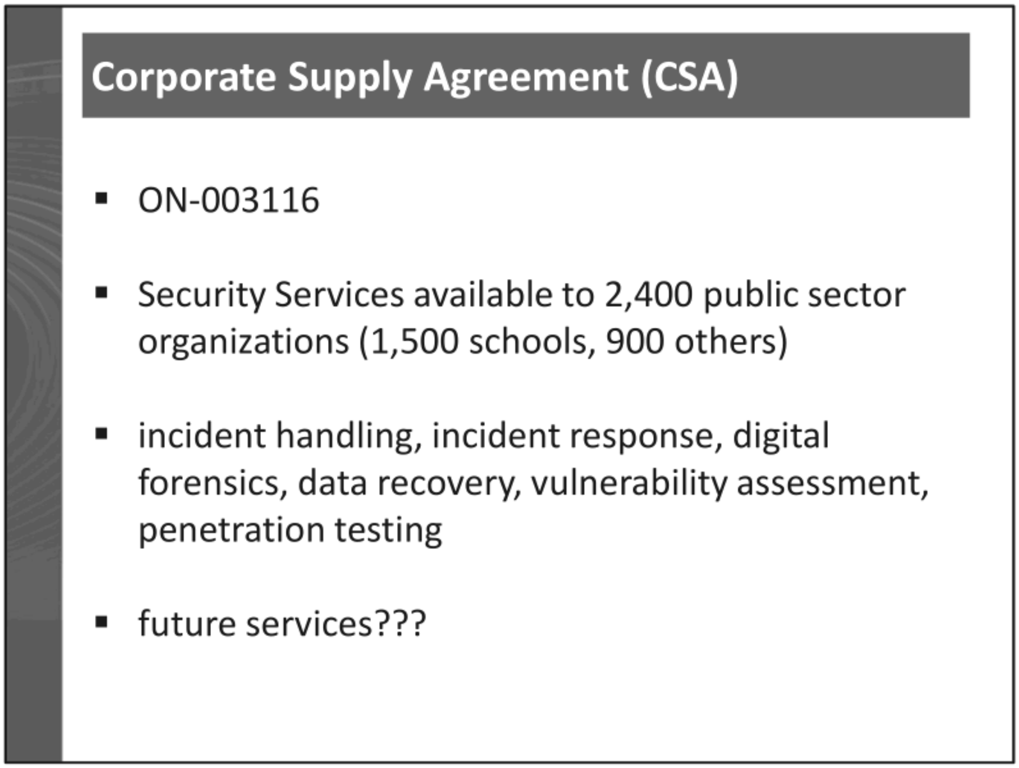
ORGANIZATION INFORMATION		
Organization Name:		
Organization Phone:		
Organization Address:		
City:	Province:	Postal Code:
Public Sector Organization? ☐ Yes ☐ No	Critical Infrastructure? ☐ Yes ☐ No	Industry:
ASN(s):	Network (s):	Domains/Websites:
BUSINESS CONTACT INFORMATION		
Name:		
Title:		
Phone:	E-mail:	Fax:
TECHNICAL CONTACT INFORMATION		
Name:		
Title:		
Phone:	E-mail:	Fax:

External Security Services



EMERGENCY CONTACT INFORMATION		
Name:		
Title:		
Phone:	E-mail:	Fax:
SERVICES		
☒ Emergency Notification	☒ Annual Survey	□ Awareness Program
□ Vulnerability Notifications	□ Security Portal Access	□ Thought Papers
□ Defensible Security Newsletter	□ Defensible Security Conference Calls	□ Defensible Security Consulting
□ Information Sharing Face-to-Face	□ Information Sharing Conference Calls	□ Security Awareness Course
□ Security News Digest/Security Day	□ Security Officer Newsletter	□ Threat Level Notifications
□ Port Scanning	□ Network Vulnerability Scanning Lite	□ Web App Scanning Lite
□ Website Monitoring Lite	□ Domain Monitoring	□ Incident Response Drill
□ Threat Intelligence Sharing (future)	□ Log Aggregation (future)	□ Self-serve Web App Scanning (future)
ACKNOWLEDGEMENT		
The information provided above is accurate to the best of my knowledge. I am a representative of the organization and am authorized to request these services. I understand that no support will be provided for the above services.		
Name (print):		Date:

Please return the completed form to OCIOSecurity@gov.bc.ca. Incomplete forms will not be accepted.

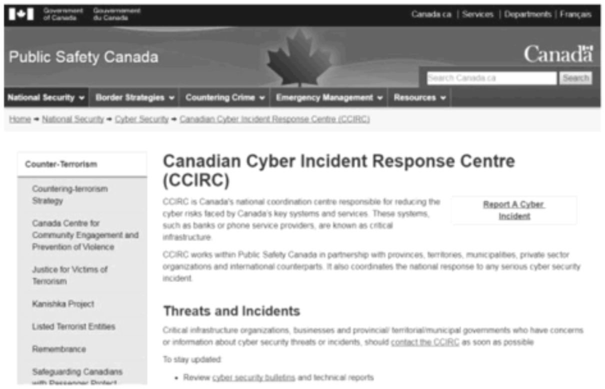


Corporate Supply Agreement (CSA)

- ON-003116
- Security Services available to 2,400 public sector organizations (1,500 schools, 900 others)
- incident handling, incident response, digital forensics, data recovery, vulnerability assessment, penetration testing
- future services???

Public Safety - CCIRC

- contact in the event of an incident, will assist
- perform malware reverse engineering
- able to sanitize info and share with others
- Cyber Resilience Review
- call them and provide your networks


Government of Canada
Gouvernement du Canada
Canada.ca | Services | Departments | Français
Public Safety Canada
Canada
Search Canada.ca
Search
National Security
Border Strategies
Countering Crime
Emergency Management
Resources
Home → National Security → Cyber Security → Canadian Cyber Incident Response Centre (CCIRC)
Counter-Terrorism
Countering-terrorism Strategy
Canada Centre for Community Engagement and Prevention of Violence
Justice for Victims of Terrorism
Kanishka Project
Listed Terrorist Entities
Remembrance
Safeguarding Canadians with Passenger Protect
Report A Cyber Incident

Canadian Cyber Incident Response Centre (CCIRC)

CCIRC is Canada's national coordination centre responsible for reducing the cyber risks faced by Canada's key systems and services. These systems, such as banks or phone service providers, are known as critical infrastructure.

CCIRC works within Public Safety Canada in partnership with provinces, territories, municipalities, private sector organizations and international counterparts. It also coordinates the national response to any serious cyber security incident.

Threats and Incidents

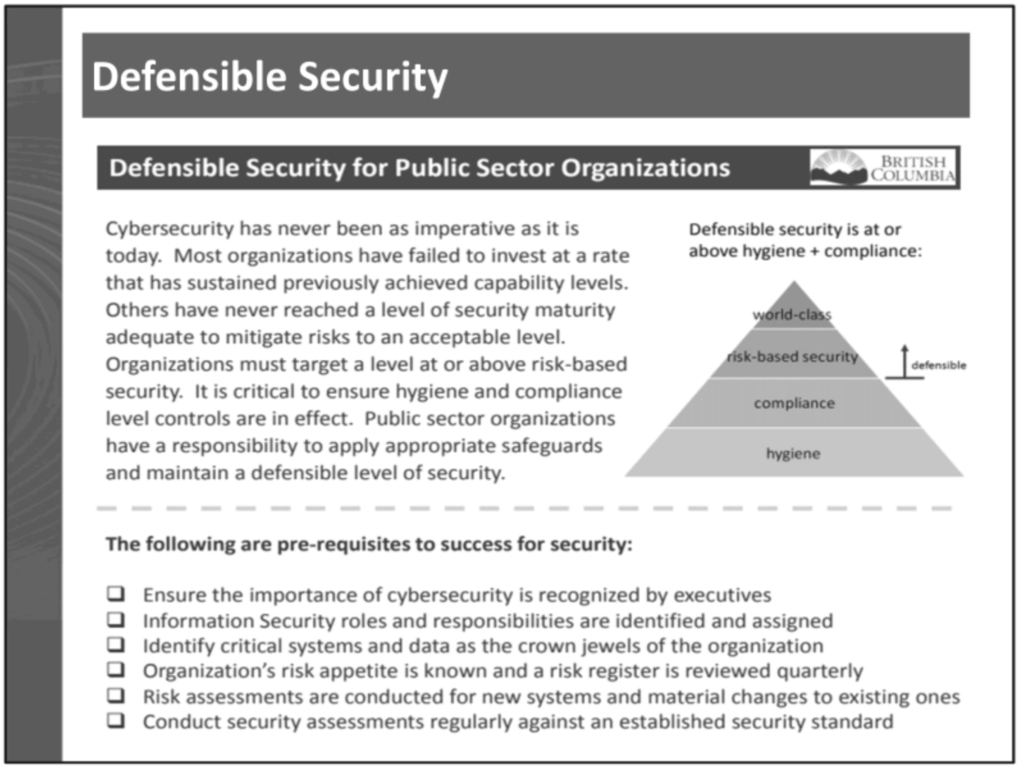
Critical infrastructure organizations, businesses and provincial/ territorial/municipal governments who have concerns or information about cyber security threats or incidents, should contact the CCIRC as soon as possible.

To stay updated:

- Review cyber security bulletins and technical reports

BEhavioural Analysis using Virtualization and Experimental Research (BEAVER)

GeekWeek
Oct 18 – Oct 26



Defensible Security

Defensible Security for Public Sector Organizations

BRITISH COLUMBIA

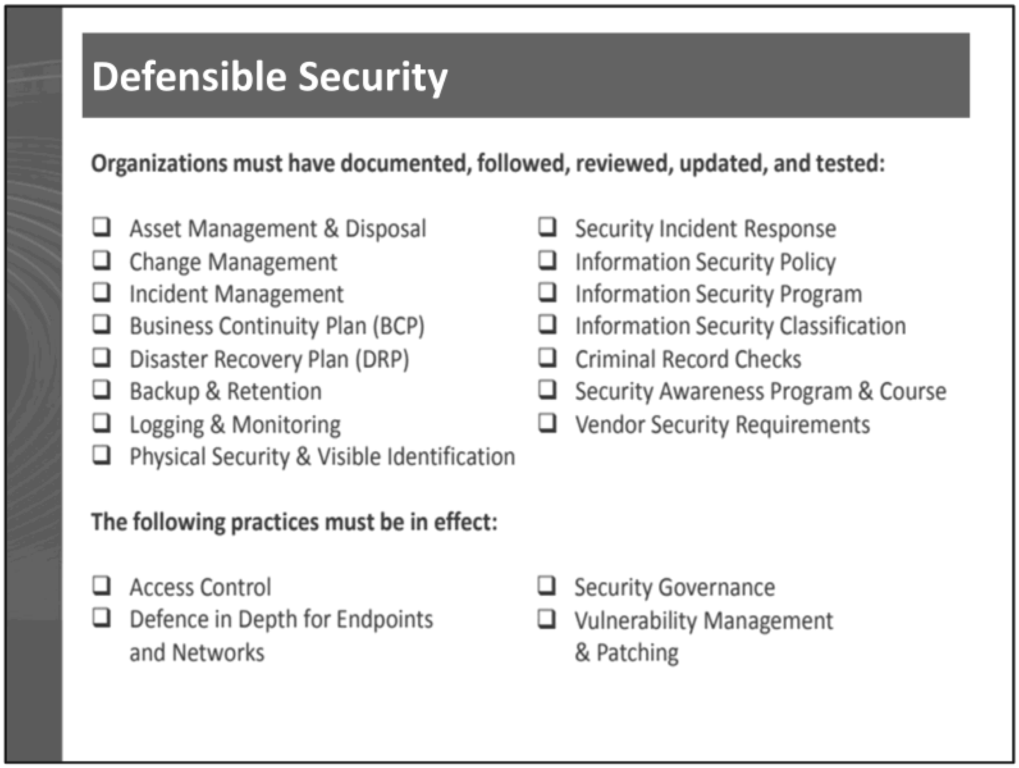
Cybersecurity has never been as imperative as it is today. Most organizations have failed to invest at a rate that has sustained previously achieved capability levels. Others have never reached a level of security maturity adequate to mitigate risks to an acceptable level. Organizations must target a level at or above risk-based security. It is critical to ensure hygiene and compliance level controls are in effect. Public sector organizations have a responsibility to apply appropriate safeguards and maintain a defensible level of security.

Defensible security is at or above hygiene + compliance:

world-class
risk-based security
compliance
hygiene
defensible

The following are pre-requisites to success for security:

❑ Ensure the importance of cybersecurity is recognized by executives
❑ Information Security roles and responsibilities are identified and assigned
❑ Identify critical systems and data as the crown jewels of the organization
❑ Organization’s risk appetite is known and a risk register is reviewed quarterly
❑ Risk assessments are conducted for new systems and material changes to existing ones
❑ Conduct security assessments regularly against an established security standard



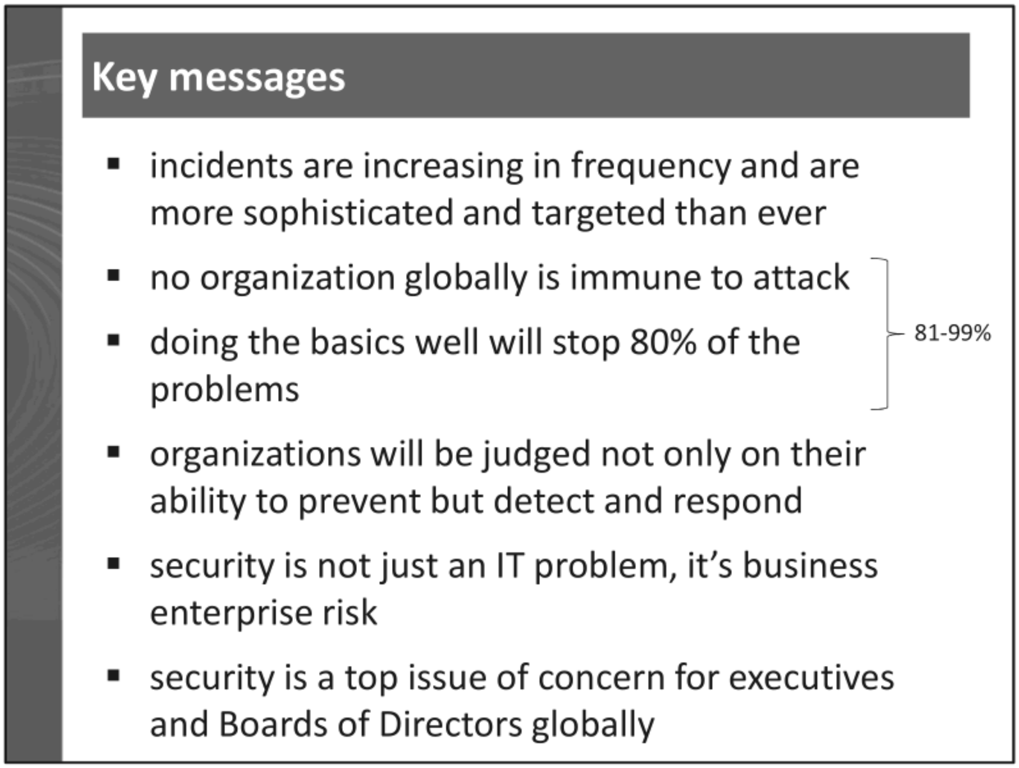
Defensible Security

Organizations must have documented, followed, reviewed, updated, and tested:

- □ Asset Management & Disposal
- □ Change Management
- □ Incident Management
- □ Business Continuity Plan (BCP)
- □ Disaster Recovery Plan (DRP)
- □ Backup & Retention
- □ Logging & Monitoring
- □ Physical Security & Visible Identification
- □ Security Incident Response
- □ Information Security Policy
- □ Information Security Program
- □ Information Security Classification
- □ Criminal Record Checks
- □ Security Awareness Program & Course
- □ Vendor Security Requirements

The following practices must be in effect:

- □ Access Control
- □ Defence in Depth for Endpoints and Networks
- □ Security Governance
- □ Vulnerability Management & Patching

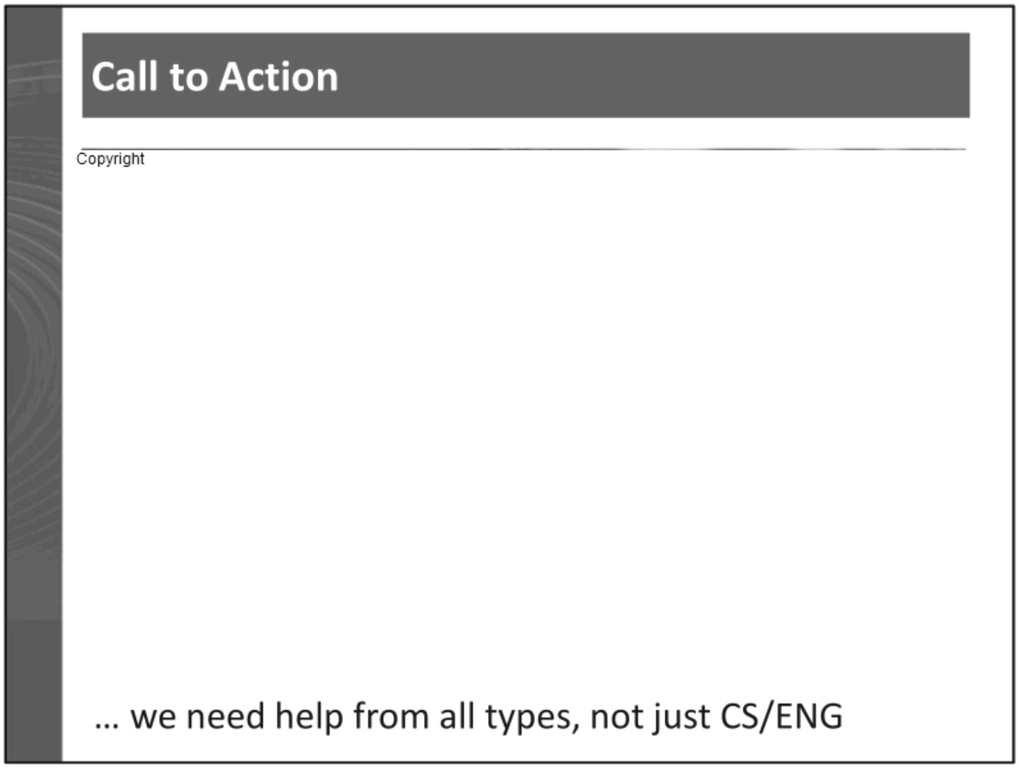


Key messages

- incidents are increasing in frequency and are more sophisticated and targeted than ever
- no organization globally is immune to attack
- doing the basics well will stop 80% of the problems

81-99%

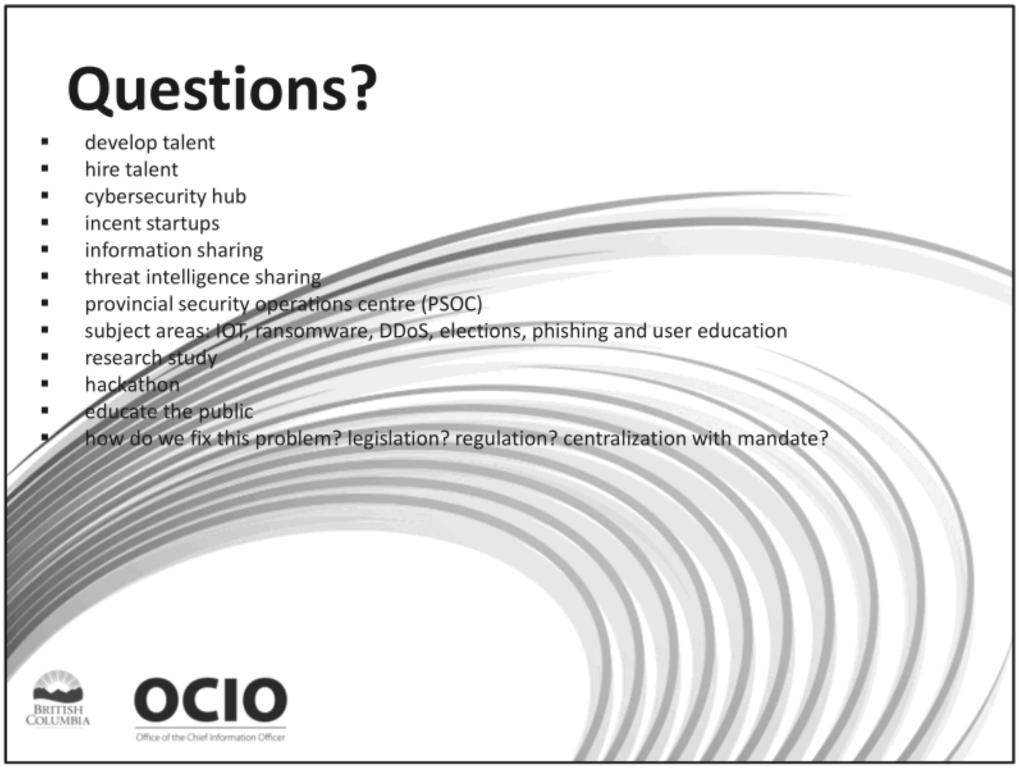
- organizations will be judged not only on their ability to prevent but detect and respond
- security is not just an IT problem, it's business enterprise risk
- security is a top issue of concern for executives and Boards of Directors globally



Call to Action

Copyright

… we need help from all types, not just CS/ENG

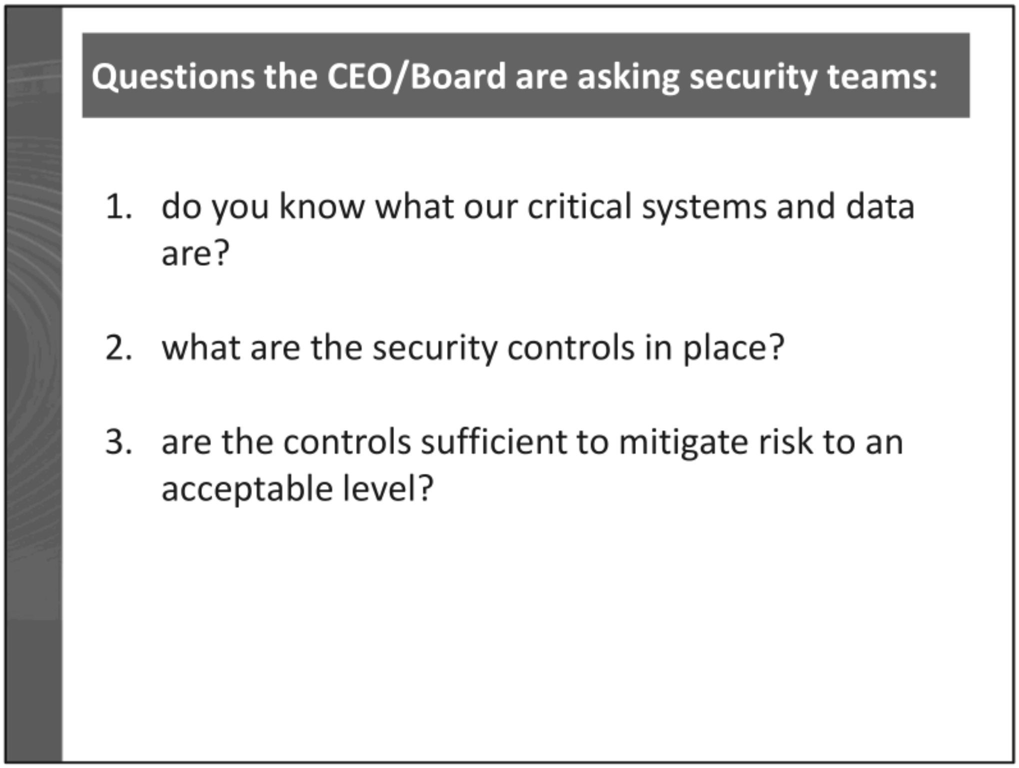


Questions?

- develop talent
- hire talent
- cybersecurity hub
- incent startups
- information sharing
- threat intelligence sharing
- provincial security operations centre (PSOC)
- subject areas: IOT, ransomware, DDoS, elections, phishing and user education
- research study
- hackathon
- educate the public
- how do we fix this problem? legislation? regulation? centralization with mandate?

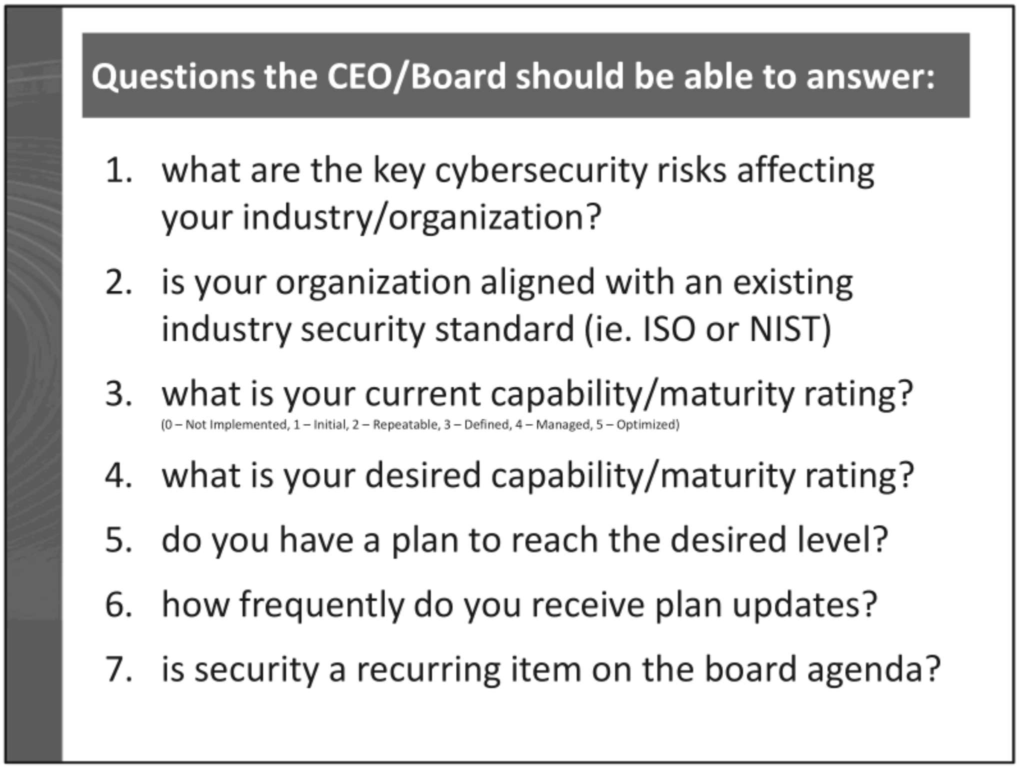
BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer



Questions the CEO/Board are asking security teams:

1. do you know what our critical systems and data are?
2. what are the security controls in place?
3. are the controls sufficient to mitigate risk to an acceptable level?



Questions the CEO/Board should be able to answer:

1. what are the key cybersecurity risks affecting your industry/organization?
2. is your organization aligned with an existing industry security standard (ie. ISO or NIST)
3. what is your current capability/maturity rating?
(0 – Not Implemented, 1 – Initial, 2 – Repeatable, 3 – Defined, 4 – Managed, 5 – Optimized)
4. what is your desired capability/maturity rating?
5. do you have a plan to reach the desired level?
6. how frequently do you receive plan updates?
7. is security a recurring item on the board agenda?