Cybersecurity Policies and Best Practices:

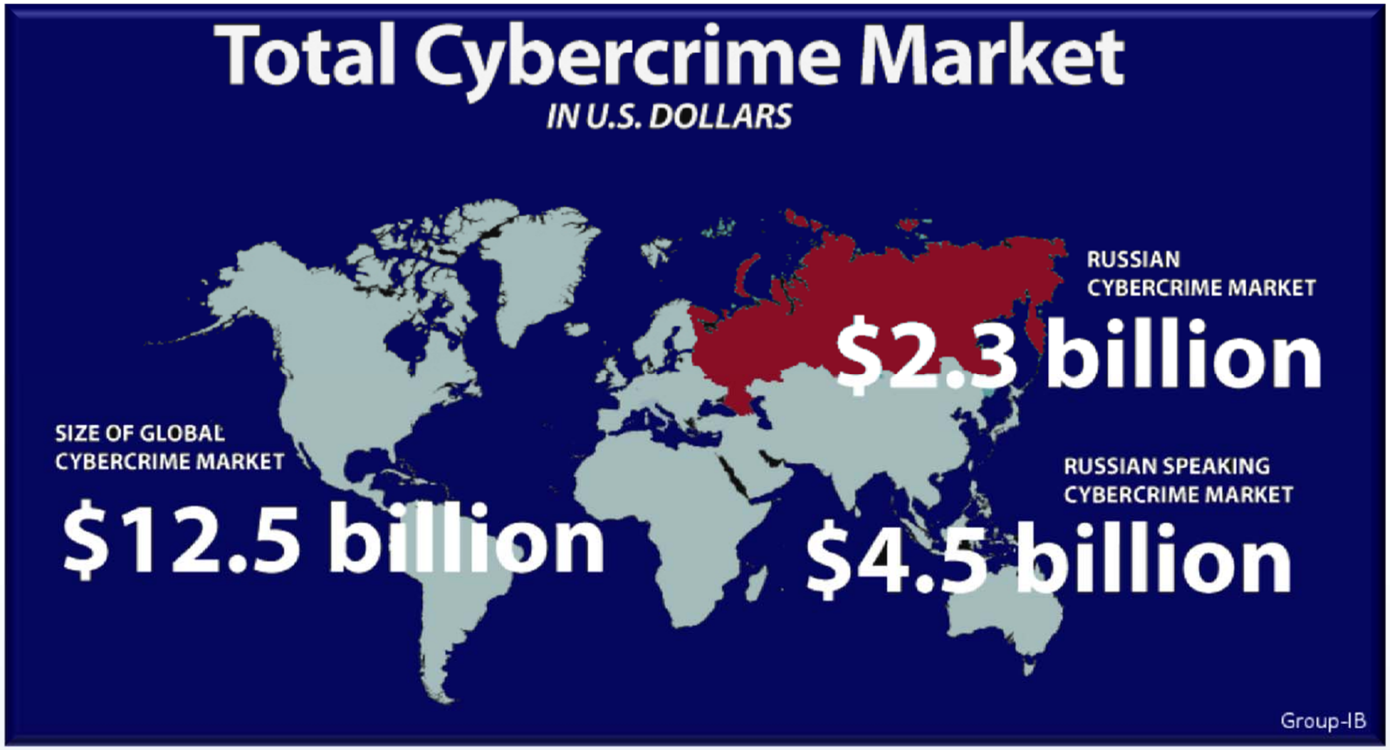
Protecting small firms, large firms, and professional services from malware and other cyber-threats

Cybersecurity Policy for Small Firms

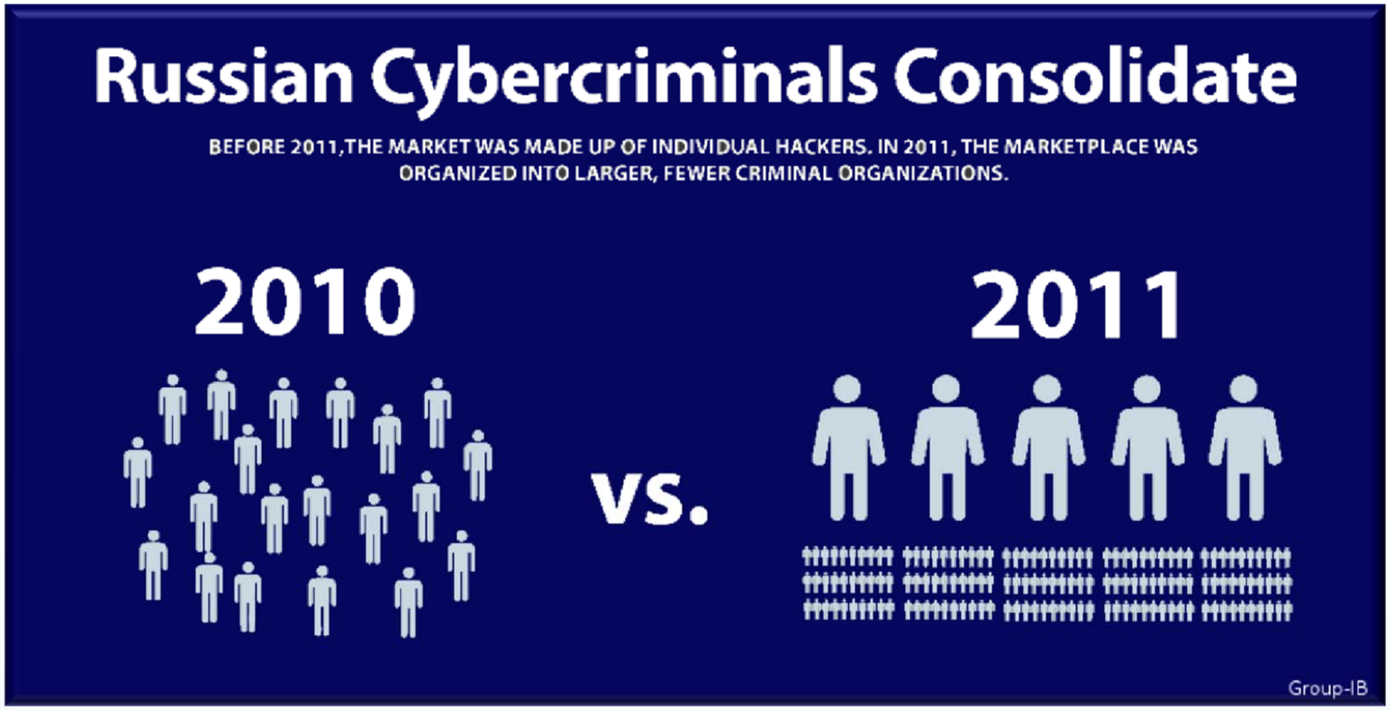
- Why is malware now a bigger threat to smaller firms than ever?
- How does cybersecurity policy help you defend your firm, employees, partners, customers?
- How does policy get made and managed?
- BONUS TIP: How cybersecurity policy can help you gain new business

Cybercrime is now a business

Cybercrime is now big business


Total Cybercrime Market
IN U.S. DOLLARS
RUSSIAN CYBERCRIME MARKET
$2.3 billion
SIZE OF GLOBAL CYBERCRIME MARKET
$12.5 billion
RUSSIAN SPEAKING CYBERCRIME MARKET
$4.5 billion
Group-IB

Well-funded and well-organized



Russian Cybercriminals Consolidate

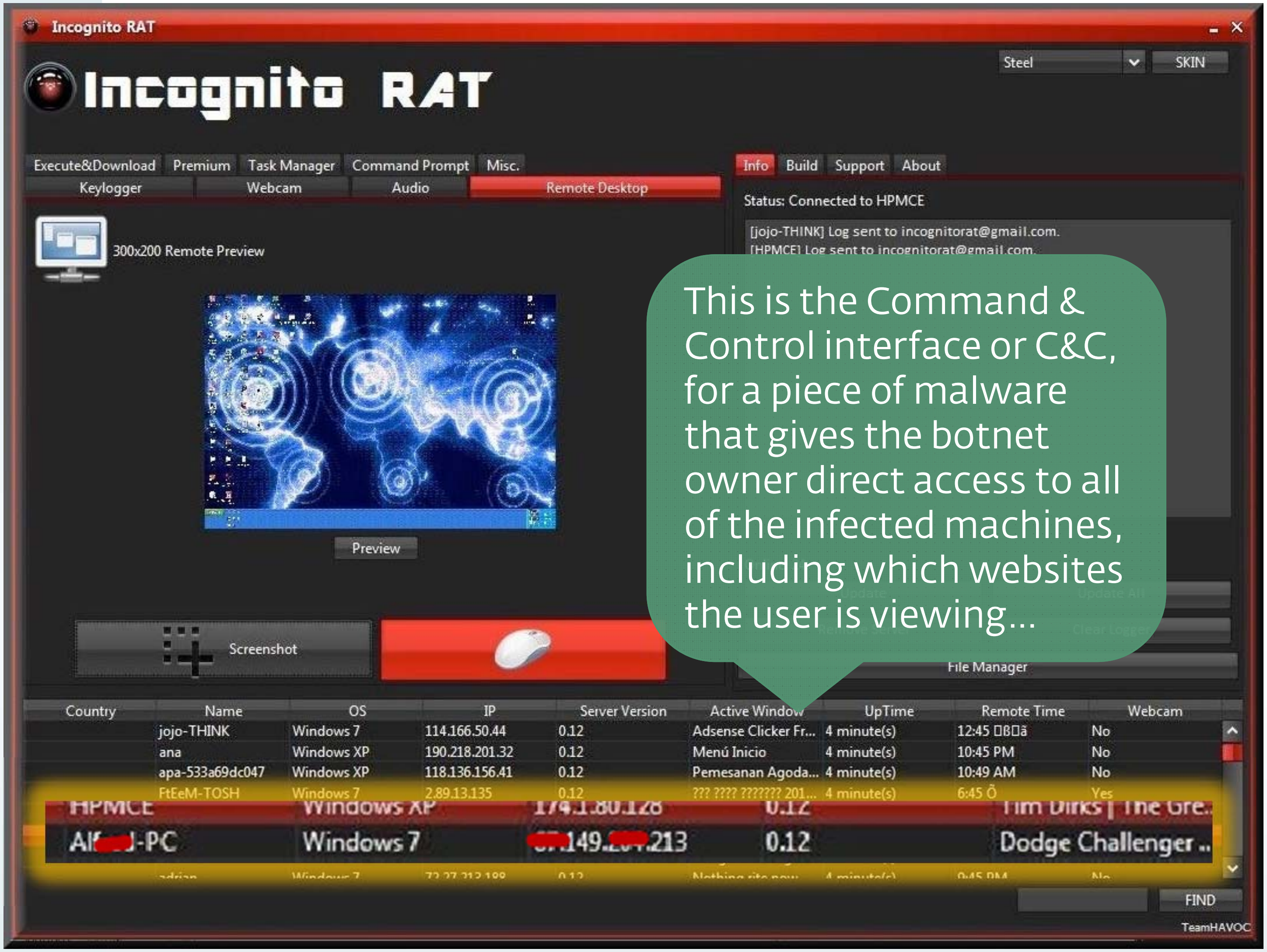
BEFORE 2011,THE MARKET WAS MADE UP OF INDIVIDUAL HACKERS. IN 2011, THE MARKETPLACE WAS ORGANIZED INTO LARGER, FEWER CRIMINAL ORGANIZATIONS.

Group-IB

With powerful tools

“Once inside, malware is installed and begins collecting data. The malware is also preconfigured to send data outbound, either via FTP or email, to a webserver under the attacker’s control. The data is then sold on the black market, or, if credentials are stolen, deeper attacks are carried out against bank accounts or other systems…”

2012 Verizon Data Breach Investigations Report



Status: Connected to HPMCE

```
[jojo-THINK] Log sent to incognitorat@gmail.com.
[HPMCE] Log sent to incognitorat@gmail.com.
```

Country	Name	OS	IP	Server Version	Active Window	UpTime	Remote Time	Webcam
	jojo-THINK	Windows 7	114.166.50.44	0.12	Adsense Clicker Fr...	4 minute(s)	12:45 ᑌßᑌã	No
	ana	Windows XP	190.218.201.32	0.12	Menú Inicio	4 minute(s)	10:45 PM	No
	apa-533a69dc047	Windows XP	118.136.156.41	0.12	Pemesanan Agoda...	4 minute(s)	10:49 AM	No
	FtEeM-TOSH	Windows 7	2.89.13.135	0.12	??? ???? ??????? 201...	4 minute(s)	6:45 Ō	Yes
	HPMCE	Windows XP	174.1.80.128	0.12	Tim Dirks | The Gre..			
	Al[redacted]-PC	Windows 7	[redacted]149.[redacted].213	0.12	Dodge Challenger ..			
	adrian	Windows 7	72.27.213.188	0.12	Nothing rita now..	4 minute(s)	9:45 PM	No

This is the Command & Control interface or C&C, for a piece of malware that gives the botnet owner direct access to all of the infected machines, including which websites the user is viewing…

SMEs: Vulnerable AND targeted

- Attack vectors have multiplied
- Criminals have done the math
- Small businesses, law firms and professional service firms have bigger bank accounts and more valuable data than consumers, but they tend to spend less on security than larger enterprises.

How vulnerable are small firms?

- **Fewer layers of protection**
- **Less in-house IT expertise**
- **Lower levels of awareness**
- **Fewer cybersecurity policies**

How targeted are small firms?

- 72% of the 855 data breaches world-wide last year were at companies with 100 or fewer employees.
- Based on analysis in the Verizon Data Breach Investigation Report

How targeted are law firms?

- “We have seen over the last three years an increase in the targeting of law firms. As client companies become targets, their security becomes stronger. Softer targets to go after are law firms.”
  - Trent Teyema, FBI assistant special agent in charge of cybercrimes, Washington field office

How targeted are law firms?

- “There is every reason to believe that foreign governments are breaking into American law firm networks.”
  - Stewart Baker, former assistant secretary for policy at the Department of Homeland Security

How can a piece of paper help?

- TJX breach cost $2 billion
- Good password, wireless, and encryption policies would have prevented it
- A policy of “see something say something” led to apprehension of the perpetrators.

Cybersecurity policy works

1. Establish a policy, for example

   "You must use strong passwords"

2. Tell all employees about the policy
3. Reward those who follow policy
4. Punish those who don't

- Result = much better password protection than if you don't do 1-4.

Creating cybersecurity policy

- Starts at the top with buy-in from partners
- “It is the policy of Fare & Juste LLP that information, in all its forms, *written, spoken, recorded electronically or printed,* will be protected from accidental or intentional unauthorized modification, or destruction throughout its life cycle.”

Policy requires controls

- The equipment and software used to process, store, and transmit information will be protected by appropriate controls.

Policies and controls

- **Policy**: All systems will be protected against malicious code that can steal, damage, or destroy information
- **Control**: Approved antivirus software will be installed on all systems

Procedures and deployment

- Procedures
  - Antivirus software will be set to update automatically. Employees are not permitted to turn off antivirus. All USB drives must be scanned for viruses.
- Deployment
  - You must make all employees **aware** of the policy and **train** them how to comply with the procedures

Enforcement and consequences

- Failure to enforce policies defeats their purpose AND negates some of the protection they provide.
- Harder to fire someone for turning off antivirus if people are routinely allowed to turn off antivirus without consequences

Templates and aggregation

- There are policy templates out there that you can adapt
- You can build policy over time, starting with the basics, adding as able or as needed

Cybersecurity policies can pay

- Large companies are now asking law firms for detailed assurances on information security policies and procedures as a condition of doing business
- We are likely to see more of this, not less

Cybersecurity policies can pay

- Do you have security policies on XYZ?
- Are your employees aware of these policies?
- If you have cybersecurity policies in place and employees educated about them, you can win business when competing with firms that are behind the curve

Defense Strategies: 3 Tips

1. Make sure you have the right policies in place AND your employees are trained

2. Educate employees AND family members about threats and defenses

3. Do your best to stay on top of patching and antivirus updates

Defense Strategies: 2 More Tips

1. Maintain control over all devices outside the office and only use encrypted wireless connections
2. Encrypt sensitive documents, when emailing, storing, or transporting them (consider a secure file transfer solution like BISCOM)

Recap: From policies to protection…

- You can defeat cyber-criminals
- Or at least make them move on to an easier target
- But defenses need to be built on a firm foundation of policies that are set by partners and upheld by employees

Remember

- Policies can’t make people do the right thing
- Policies can help people **do the right things** and **avoid the wrong things**.
- Policies are the foundation of your cybersecurity strategy
- Policies need to be: documented, taught, audited, and enforced!

Thank you!

- Stephen Cobb, CISSP
- ESET Security Evangelist
- Visit www.eset.com
- Subscribe to blog.eset.com