BÁO CÁO TỔNG QUAN
AN TOÀN THÔNG TIN VIỆT NAM 2012

Người trình bày:

Ts. Vũ Quốc Thành

Phó chủ tịch, Tổng thư ký

Hiệp hội An toàn thông tin Việt Nam (VNISA)

2011 … 2012

Chủ quyền số (Digital Sovereignty):

Canada:

+ 2011

+ 2012

Russia:

+ 11/2012

…

rbth.ru/articles/2012/11/09/russias_federation_council_takes_a_closer_look_at_cybersecurity_19977.html

Home > Society

Russia's Federation Council takes a closer look at cybersecurity

November 9, 2012 Maxim Ivanov, Kommersant

Ruslan Gattarov, người đứng đầu Ủy ban Chính sách thông tin của Hội đồng Liên bang: mục tiêu tổng thể của chiến lược là phải đảm bảo "chủ quyền số"

In the words of Ruslan Gattarov, head of the Federation Council Information Policy Commission, the overall purpose of the strategy must be to ensure Russia's "digital sovereignty."

- Russian investigators

Nội dung

1. Một số sự kiện về ATTT năm 2012
(Information Security facts in 2012)

2. Kết quả khảo sát hiện trạng ATTT 2012 của VNISA
(VNISA Research on Information Security status in 2012)

3. Kết luận
(Conclusions)

10 sự kiện nổi bật về ATTT tại Việt nam 2012 *

- Ban soạn thảo Luật An toàn thông tin số được thành lập với mục tiêu sớm đưa luật vào hoạt động***
- Thông tư Quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam bắt đầu triển khai trên thực tế
- Việt nam vẫn tiếp tục đứng vị trí cao trong nhiều danh sách quốc tế cảnh báo về các nguy cơ mất an toàn**
- Xuất hiện nhiều biến thể virus ăn cắp tài khoản ngân hàng trực tuyến. Giả mạo trang yahoo để ăn cắp mật khẩu người dùng.
- Nhiều cơ quan, tổ chức phát hiện các kết nối ngầm và các mã độc chuyên dùng để đánh cắp thông tin có chủ đích (APT)

*Không xếp thứ tự

**: top 5 về NSD Internet; 15 phát tán mã độc; 10 tin rác; 15 zombie,..*

**** Thông tư liên tịch 4 Bộ, Viên KS và Tòa Án về Bộ luật Hình sự ...*

10 sự kiện nổi bật về ATTT tại Việt nam 2012 (tiếp)

- Website một doanh nghiệp nổi tiếng về an ninh mạng bị tấn công và tiếp sau đó 2 tuần trang forum của họ lại bị tấn công tiếp
- “Nguy cơ một cuộc chiến tranh mạng đối với Việt nam là có thể xảy ra”, Bộ trưởng trả lời trước Quốc hội, chiều 14/6.
- Vấn đề rò rỉ thông tin qua các thiết bị viễn thông nhập khẩu lại được dư luận chú ý
- Vấn nạn rao bán thông tin cá nhân trên mạng chưa có giải pháp ngăn chặn
- 5-2012 VNISA đánh giá ngẫu nhiên 100 webstite tên miền .gov.vn cho thấy 78% số website có thể bị tấn công toàn diện

Kết quả khảo sát 2012 của VNISA

Khảo sát được tiến hành trong khoảng 3 tháng, thực hiện bởi VNISA và VNCERT

Tổng số phiếu trả lời đầy đủ là 507, đại diện cho 507 tổ chức với đầy đủ các thành phần

Khảo sát nhằm đánh giá mức độ nhận thức và ứng dụng ATTT trong các tổ chức, doanh nghiệp

Các nội dung chính

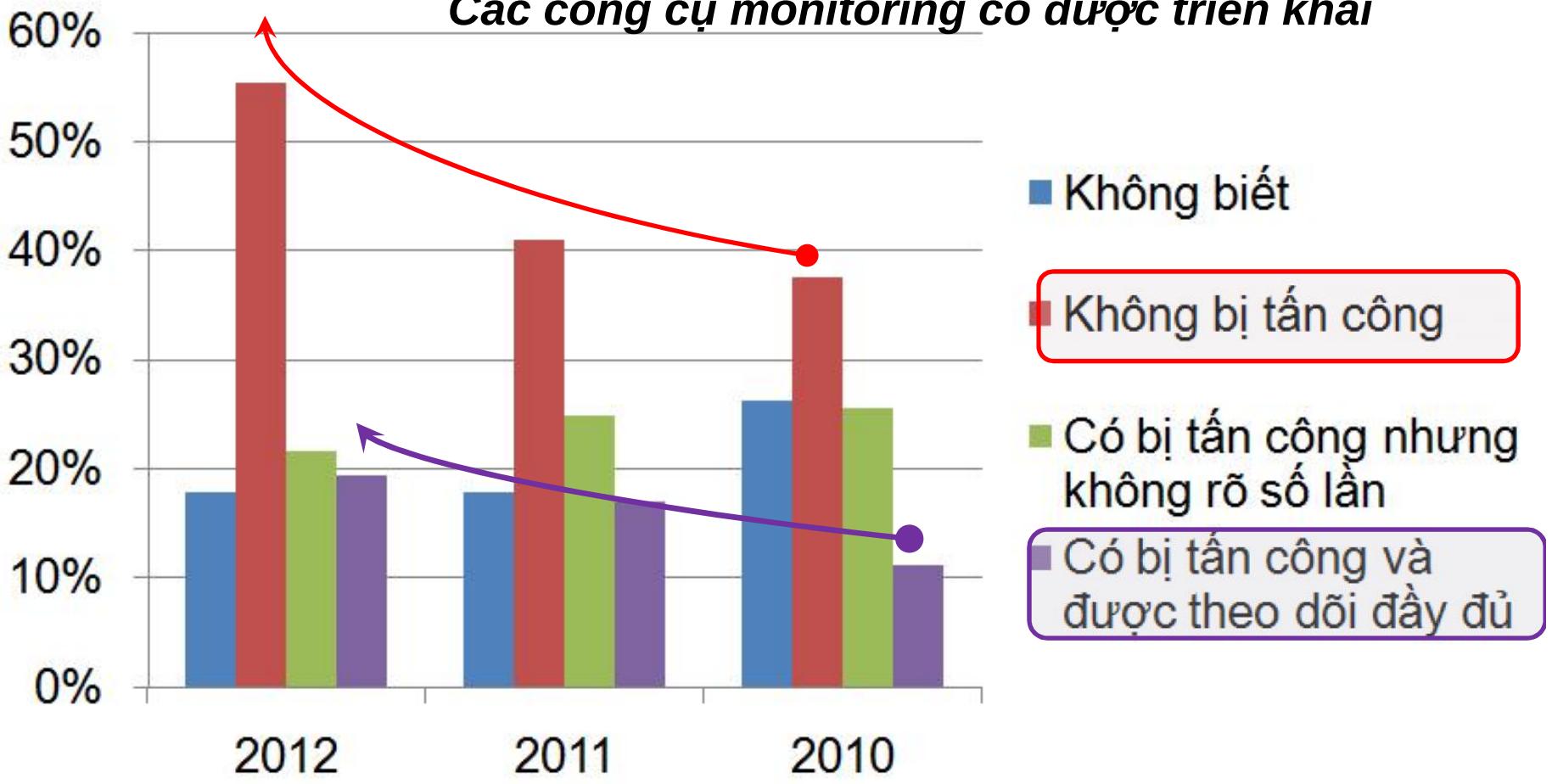
1. Nhận thức về các cuộc tấn công
2. Các biện pháp đảm bảo ATTT
3. Chi tiêu cho ATTT
4. Đào tạo về ATTT

1. Nhận thức về các cuộc tấn công

Bạn có biết mạng bị tấn công hay không?
Có ước lượng được thiệt hại không?
Có quy trình phản ứng với tấn công hay không?

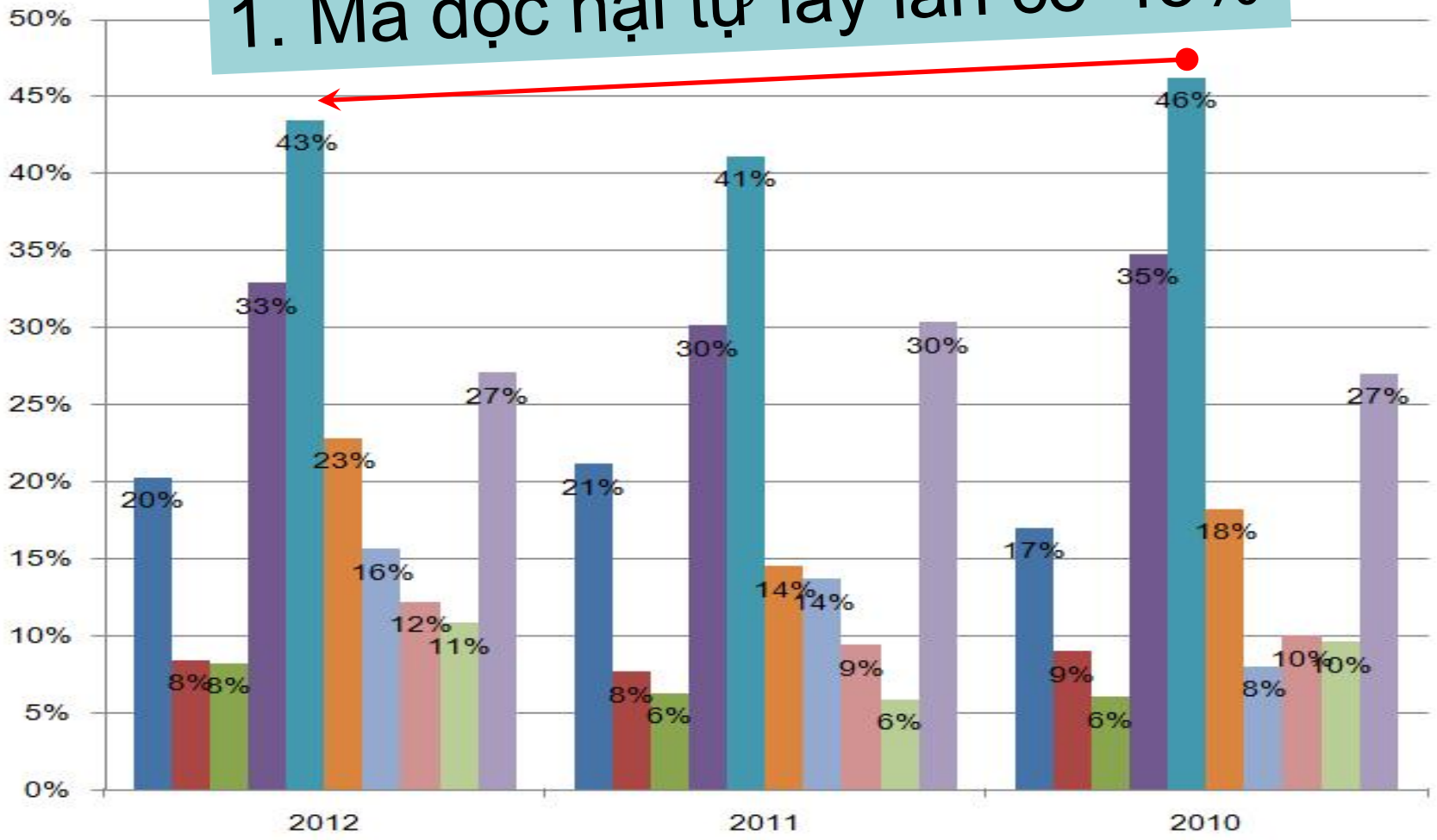
Hệ thống của quý vị đã từng bị tấn công mạng (Cyber Attack) hay không (tính từ 1/2012)?

Xu hướng nhận biết tấn công vẫn tăng qua 2 năm. Các công cụ monitoring có được triển khai

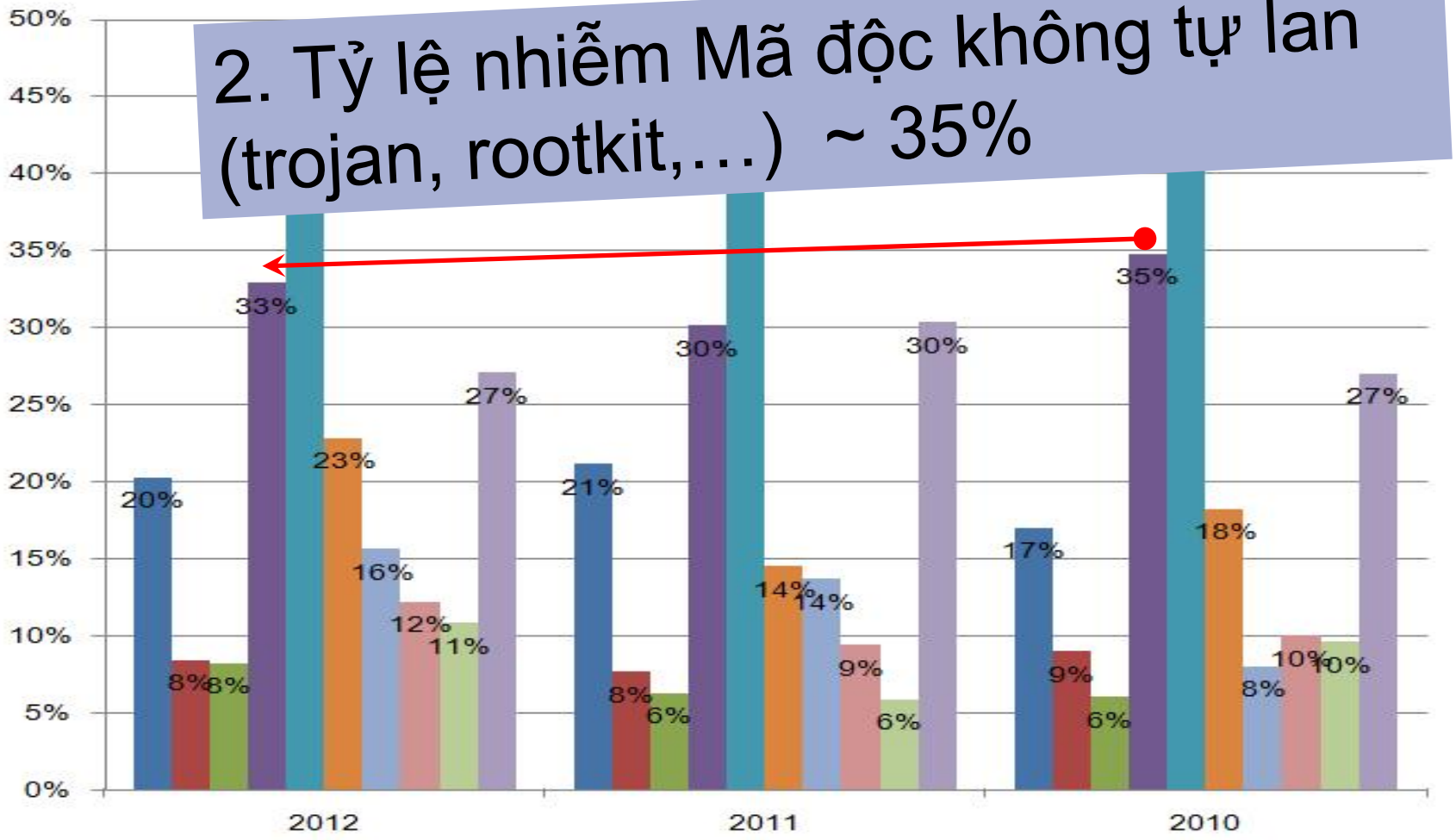


Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2012

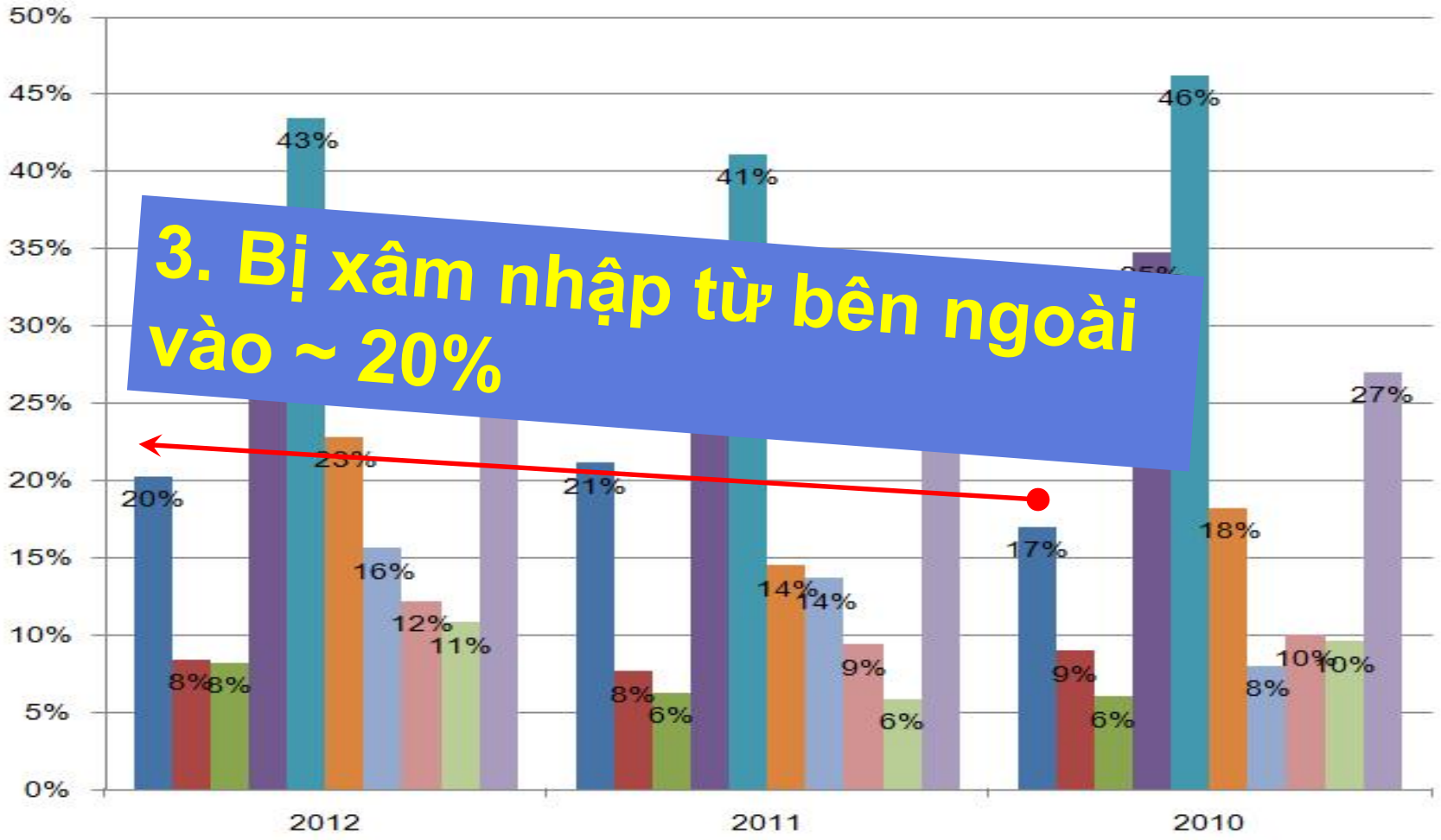
1. Mã độc hại tự lây lan cỡ 45%



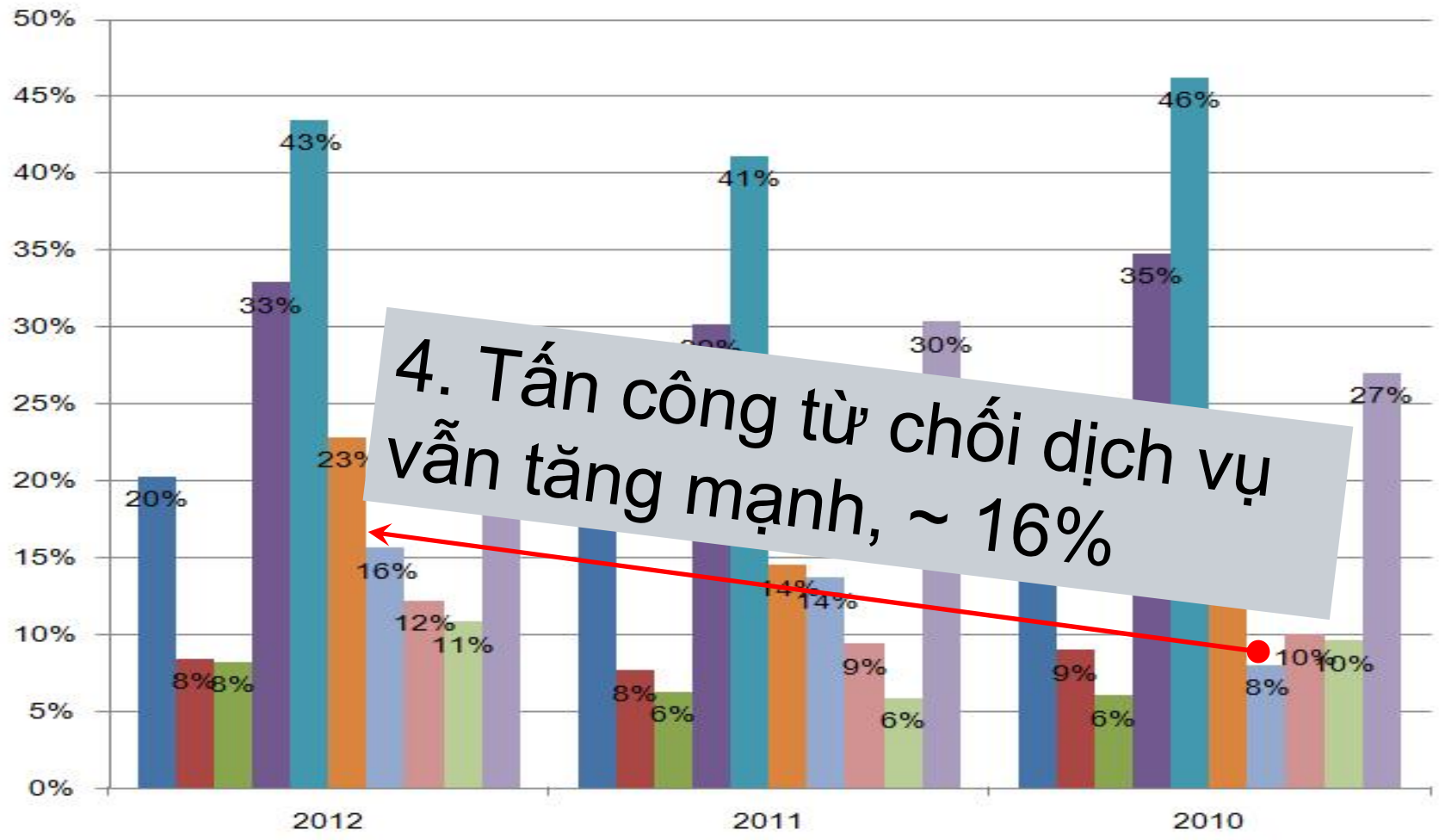
Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2012



Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2012

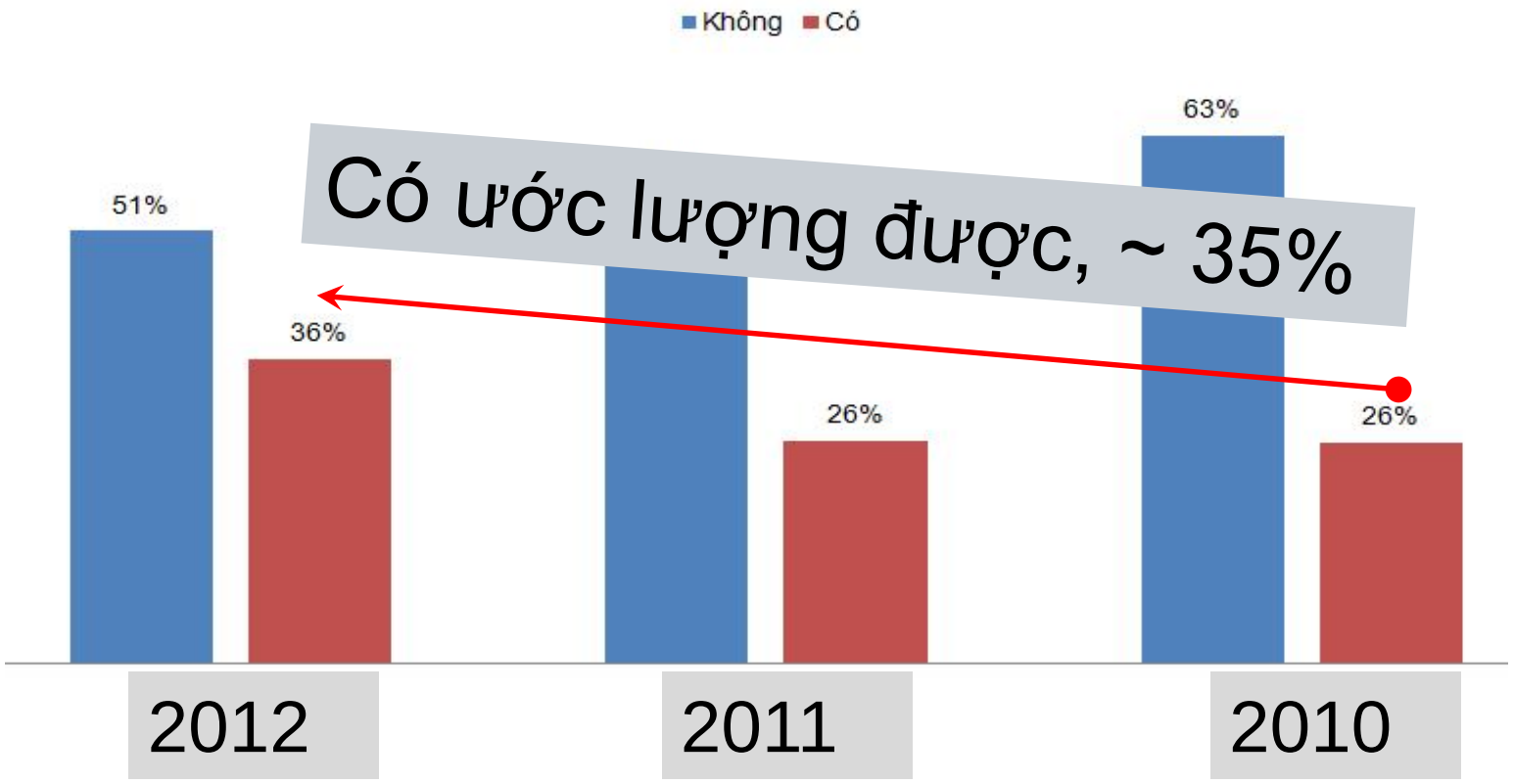


Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2012



APT (Advanced Persistent Threat):
Phá hoại có chủ đích: là động cơ hàng đầu được nhắc đến ~18%

Tổ chức của quý vị có ước lượng được tương đối tổn thất tài chính khi bị tấn công không?



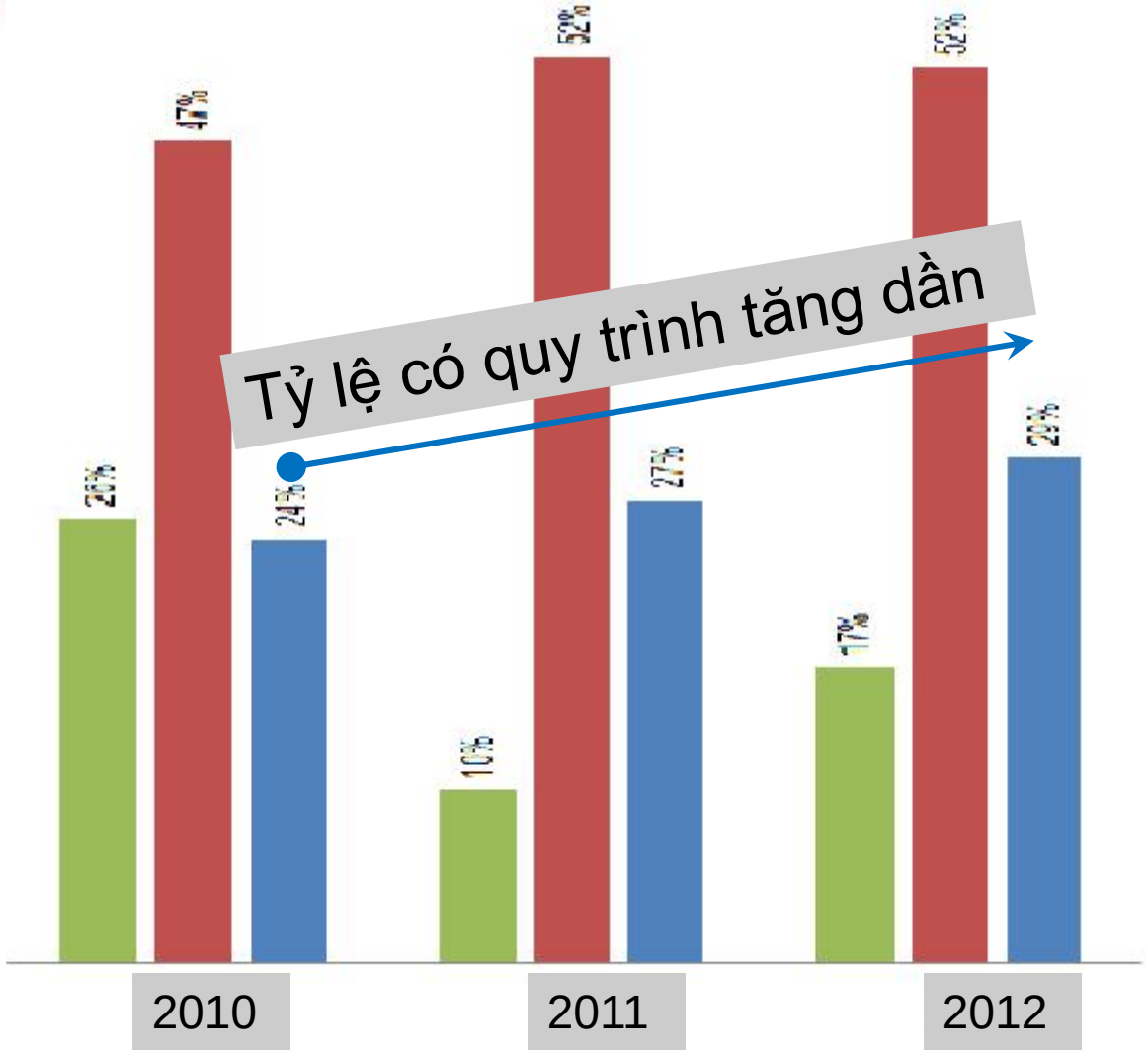
1. Khả năng đánh giá tổn thất tài chính có tăng lên

2. Đa số không rõ động cơ tấn công là gì hoặc động cơ không rõ ràng (trên 70%)

2. Các biện pháp đảm bảo ATTT

Các biện pháp quản lý: Quy trình, Quy chế, Báo cáo, ...
Các biện pháp kỹ thuật, công nghệ: tường lửa, chống xâm nhập, ...

Tổ chức của quý vị có quy trình thao tác chuẩn (Standard operating procedures) để phản hồi lại những cuộc tấn công máy tính hay không ?



Năm 2011: Tỷ lệ nói "Sẽ làm trong 3 tháng tới" tăng mạnh
2012: "chưa có kế hoạch" vẫn còn là 33%

Nếu tổ chức của quý vị bị tấn công máy tính, quý vị sẽ thông báo tin này đến ai?

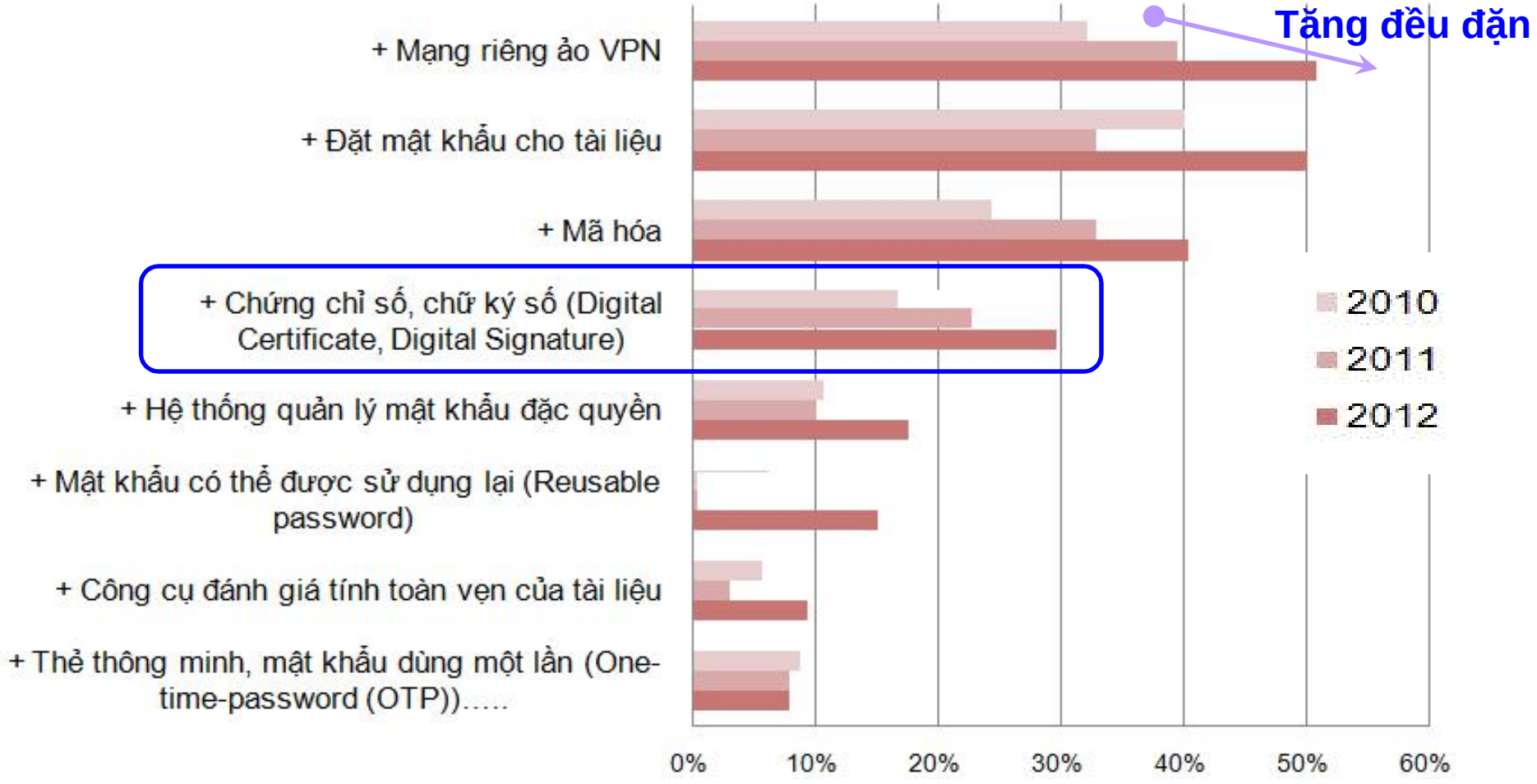
Báo cáo 2010: đa số vẫn chỉ báo cáo nội bộ, báo cáo bên ngoài tăng so với 2009

Thường sau bao lâu quý vị sẽ thông báo thông tin này?

Nhu cầu trợ giúp ngay lập tức tăng cao

Tổ chức của quý vị đang sử dụng các công nghệ đảm bảo ATTT nào?

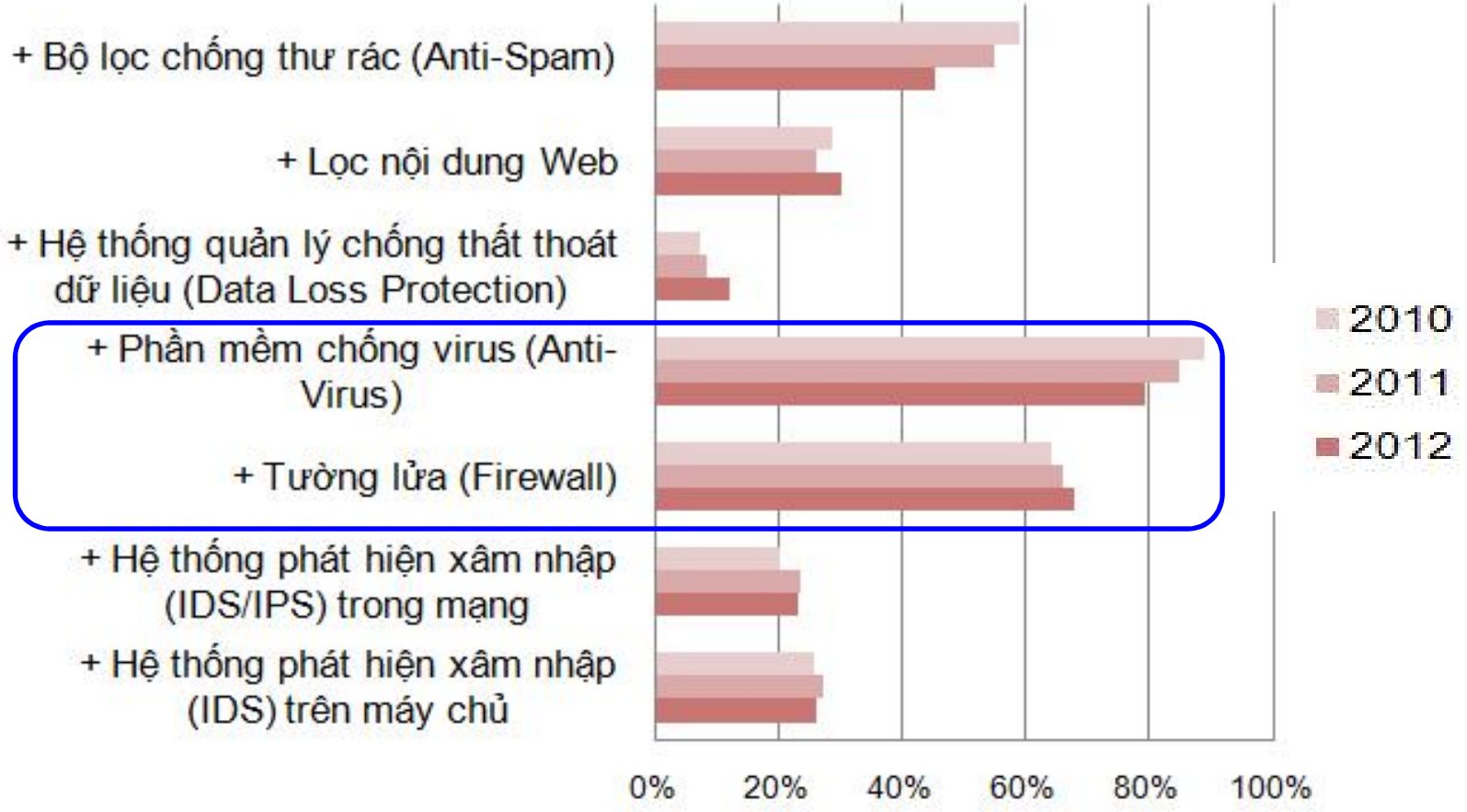
A - Nhóm bảo vệ dữ liệu bằng mật khẩu, mật mã



Sử dụng chứng chỉ số khá nhiều, OTP còn ít quá

Tổ chức của quý vị đang sử dụng các công nghệ đảm bảo ATTT nào?

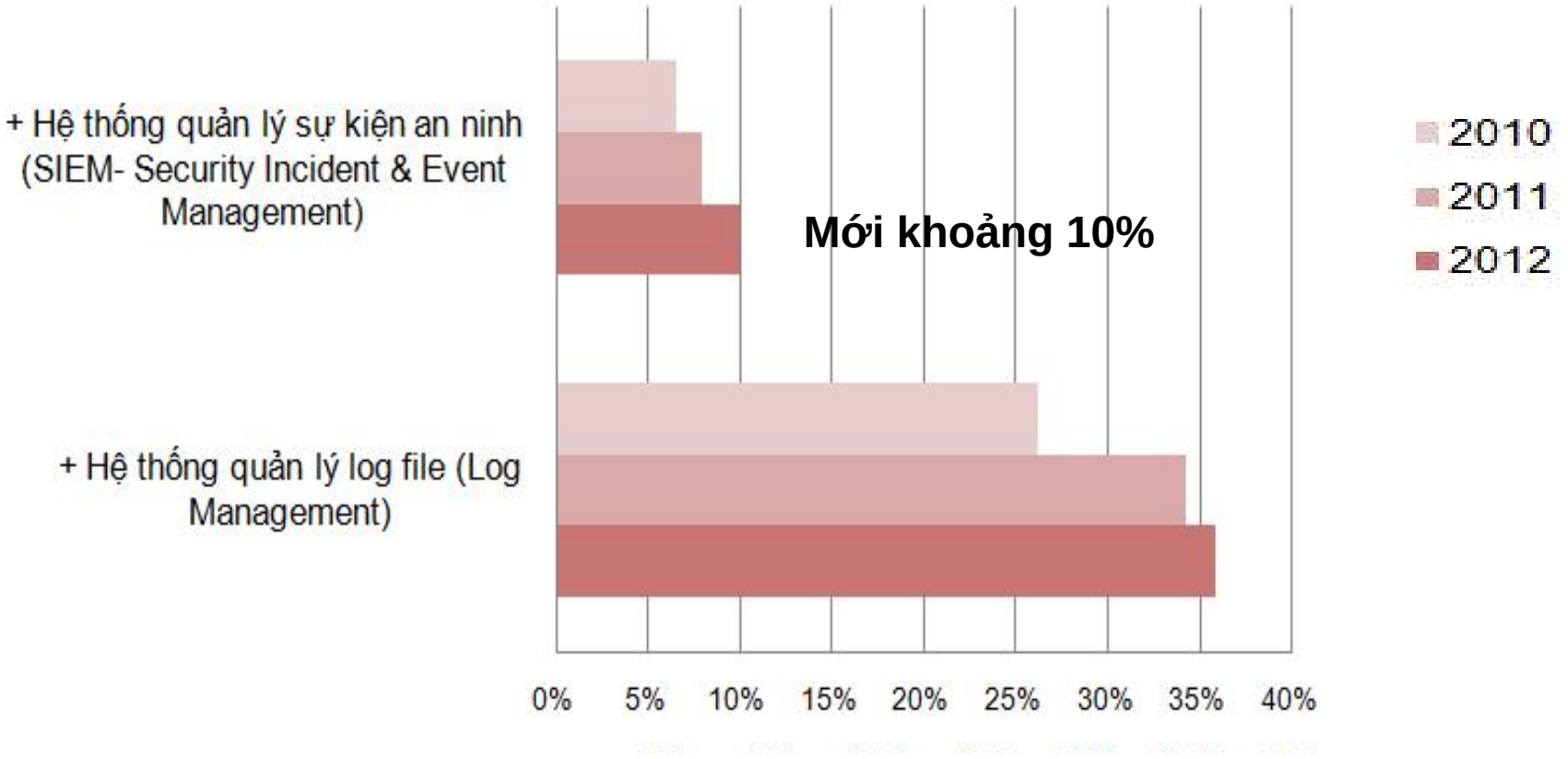
B - Nhóm bảo vệ dữ liệu bằng mật khẩu, mật mã



AV, FW, Anti-Spam sử dụng nhiều, nay chững lại

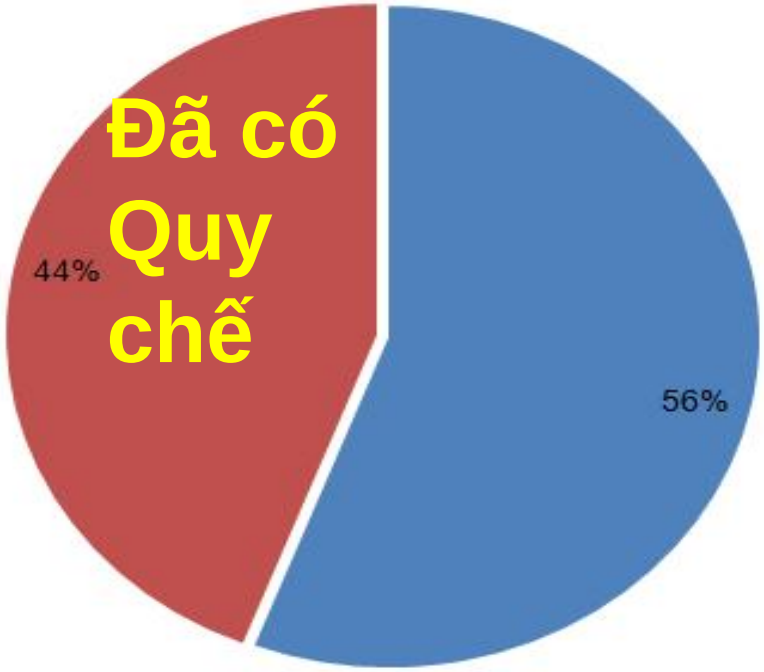
Tổ chức của quý vị đang sử dụng các công nghệ đảm bảo ATTT nào?

C - Nhóm công cụ quản lý, dò quét



Dù có tăng nhưng tỷ lệ còn quá thấp, do nhận thức chưa đầy đủ cần đẩy mạnh khuyến cáo

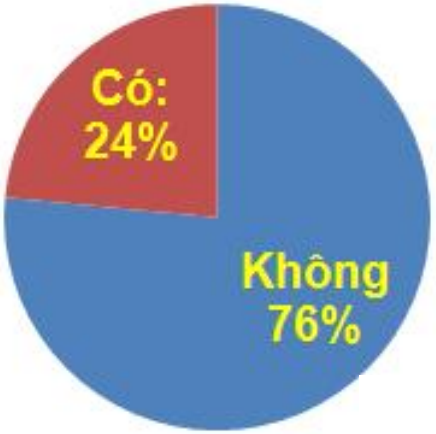
Tổ chức của quý vị có Quy chế về ATTT (Security Policy) chưa?



Tỷ lệ tăng lên so với 2011
Cần khuyến cáo bắt buộc

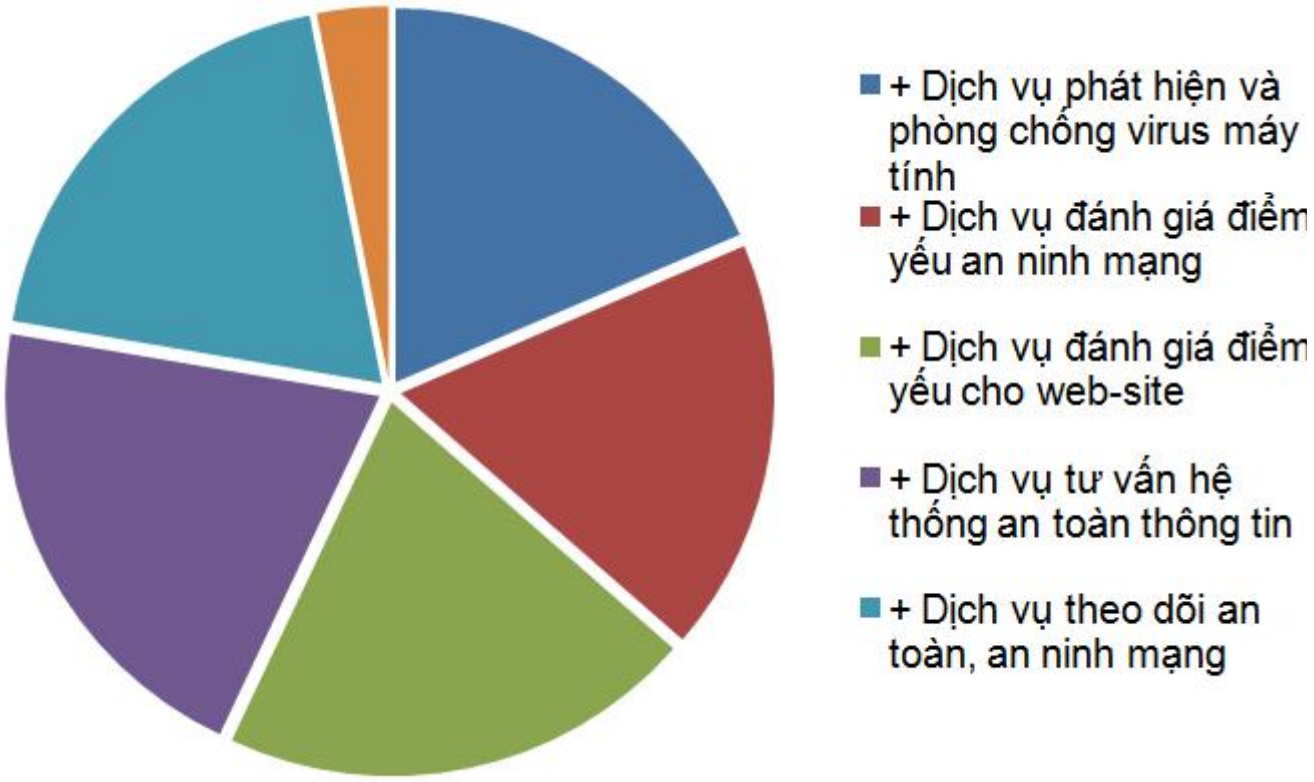
Chưa có Quy chế

Tổ chức của quí vị có dự định thuê ngoài (out-source) các dịch vụ về đảm bảo an toàn thông tin không?



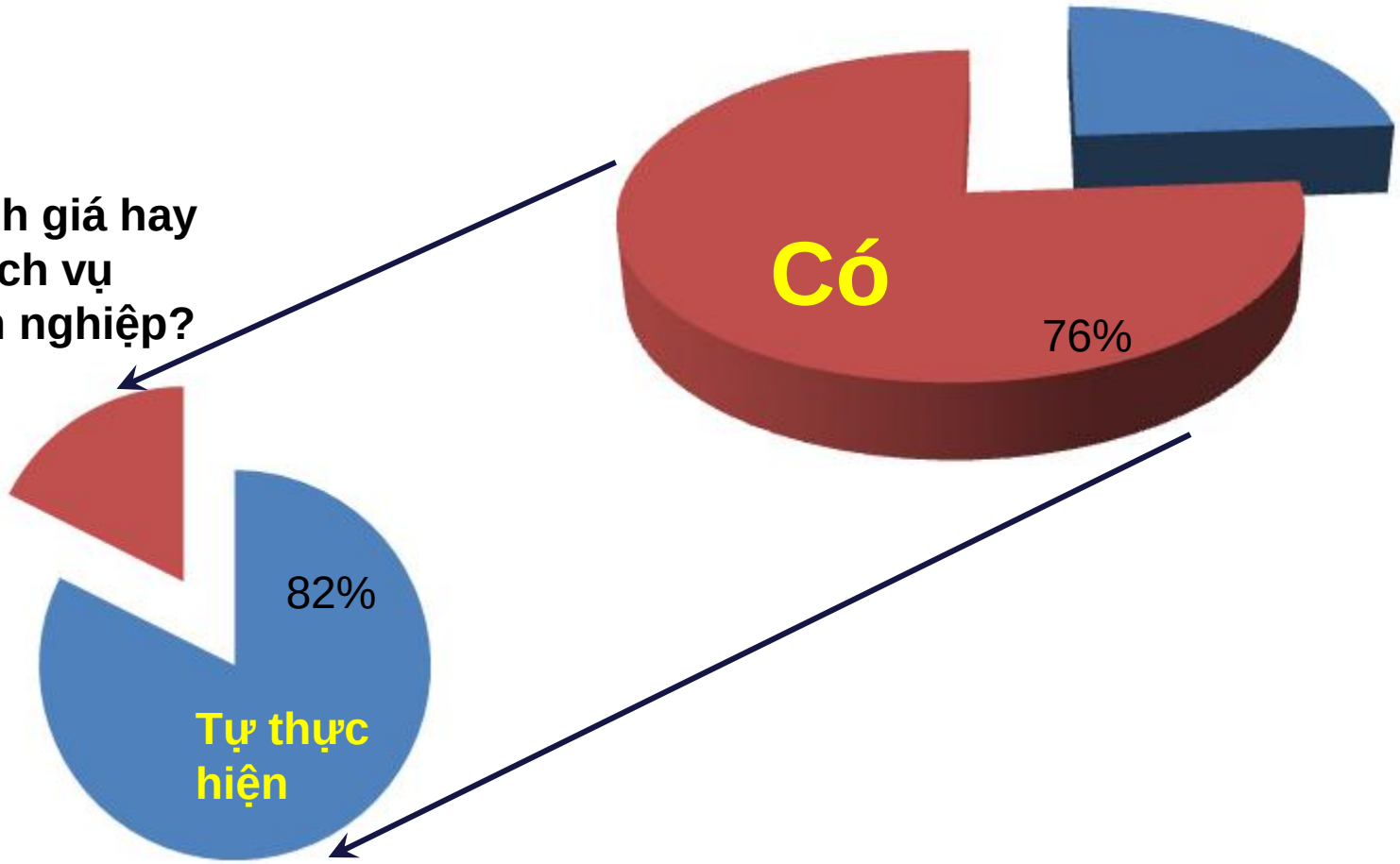
2012

Cần khuyến khích sử dụng các dịch vụ chuyên nghiệp rộng rãi hơn



Có thực hiện kiểm tra, đánh giá ATTT hay không?

Tự đánh giá hay thuê dịch vụ chuyên nghiệp?

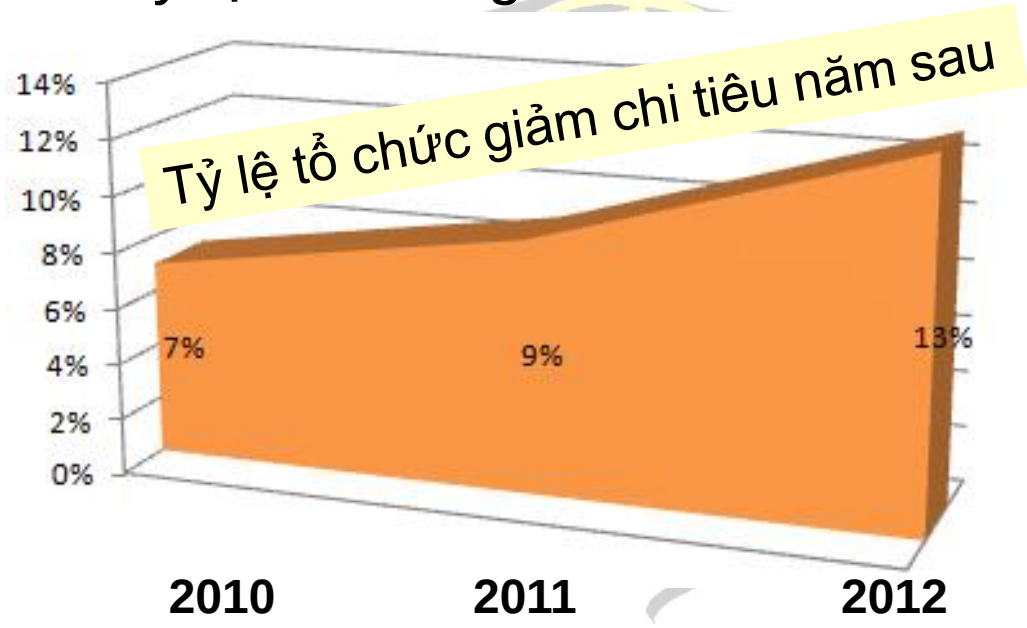


Cần tiến tới dịch vụ chuyên nghiệp và khách quan

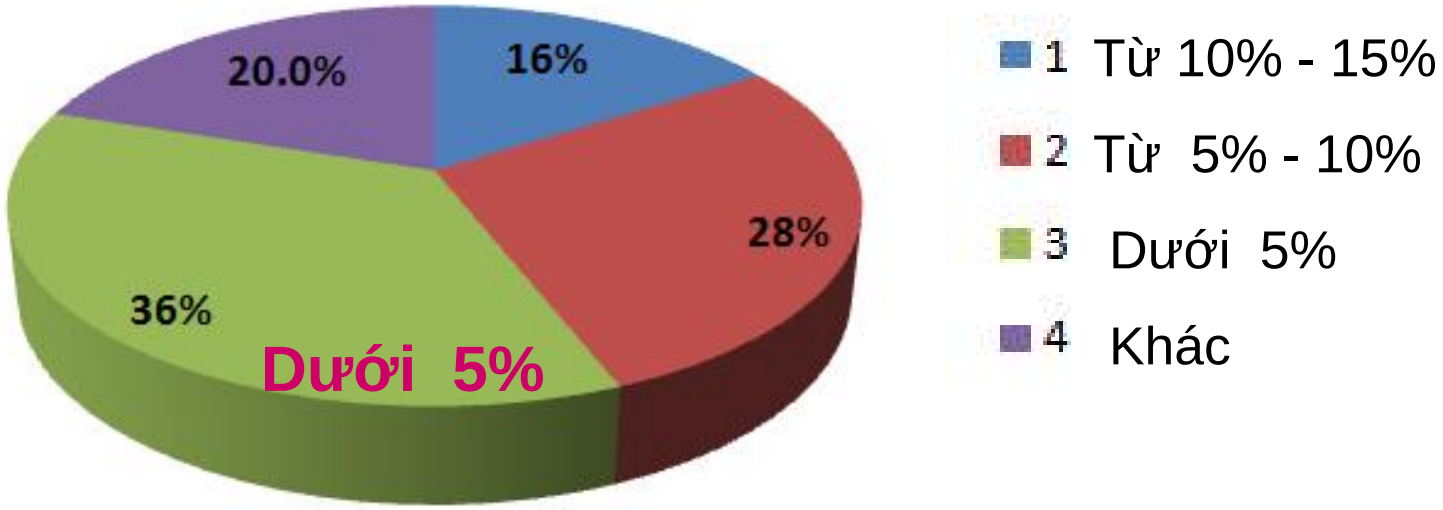
3. Chi tiêu cho ATTT – khó khăn hơn

87% cho là trong năm 2012, chi tiêu cho ATTT của tổ chức họ không giảm
57% cho rằng chi tiêu này sẽ phải tăng lên trong năm 2013

Tuy nhiên các tỷ lệ trên đã giảm khá rõ so với 2 năm trước



Tỷ lệ đầu tư cho ATTT trong ngân sách dành cho CNTT



Cảnh báo: tỷ lệ lớn chỉ dành ngân sách cho ATTT dưới 5%

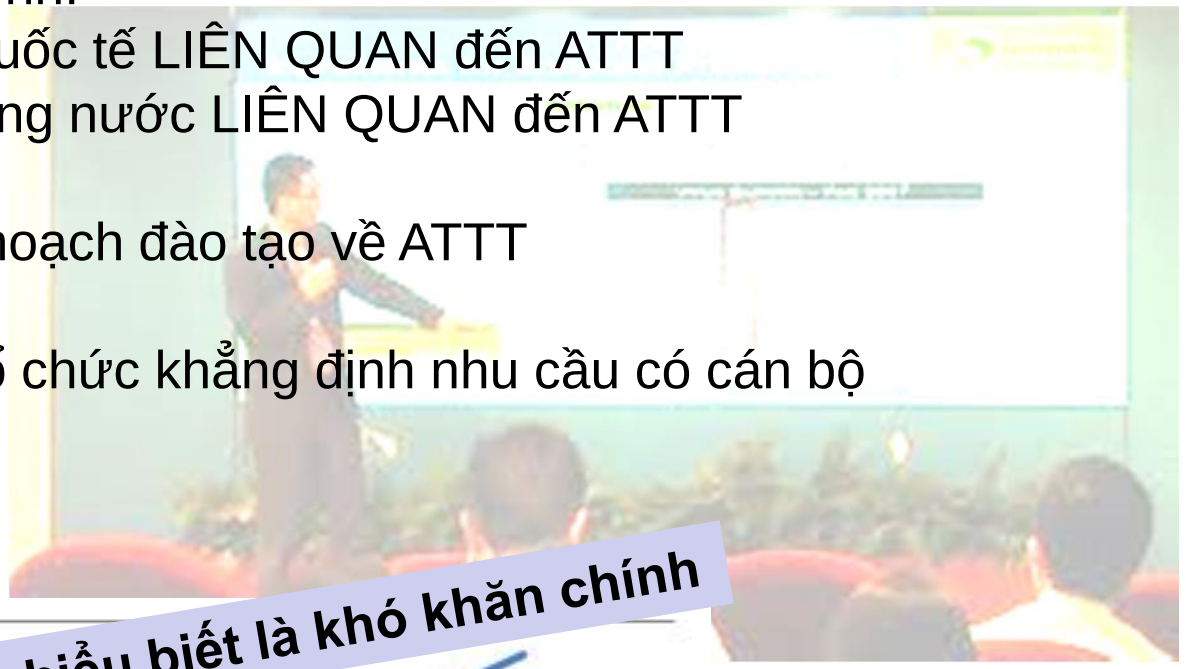
4. Nhu cầu đào tạo về ATTT

Mỗi một tổ chức có trung bình:

+ 0,89 chứng chỉ quốc tế LIÊN QUAN đến ATTT
+ 1,2 chứng chỉ trong nước LIÊN QUAN đến ATTT

Chỉ có 49% tổ chức có kế hoạch đào tạo về ATTT

Trong khi đó có đến 57% tổ chức khẳng định nhu cầu có cán bộ chuyên trách về ATTT



Kết luận

Độ đo ATTT (CIS)

FUNCTION	MANAGEMENT PERSPECTIVE	DEFINED METRICS
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean-time to incident discovery • Number of incidents • Mean-time between security incidents • Mean-time to incident recovery
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability scanning coverage • Percent of systems with no known severe vulnerabilities • Mean-time to mitigate vulnerabilities • Number of known vulnerabilities
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch policy compliance • Patch management coverage • Mean-time to patch
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of applications • Percent of critical applications • Risk assessment coverage • Security testing coverage
Configuration Management	How do changes to system configuration affect the security of the organization?	• Mean-time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions
Financial Metrics	What is the level and purpose of spending on information security?	• IT security spending as % of IT budget • IT security budget allocation

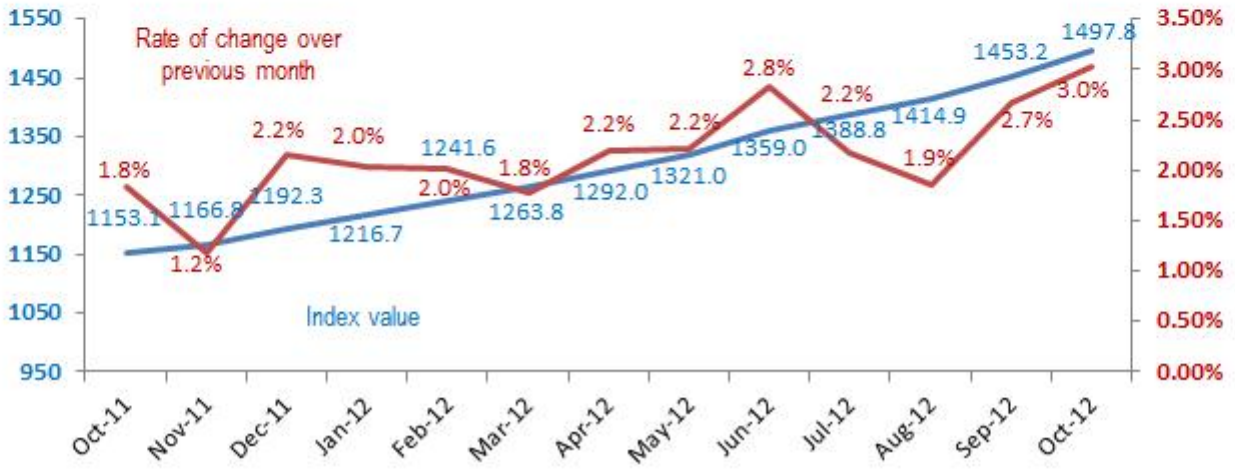
Table 1 – Center for Internet Security (CIS) Security Metrics

www.securitymetrics.org

ISO 27004

INDEX OF CYBER SECURITY

ICS VALUE, OCTOBER 2012 = 1497.8 (BASE = 1000, MARCH 2011)



Bắt đầu từ 4/2011

National Cyber Security Index

index	area	Indicators
Index for cyber safety Readiness (8 indicators)	Information security	1. establish information security policy 2. Ratio of information security budget 3. Usage of information security solution
	Personal information security	1. Counter measure & helping system for P.I 2. Exclusive division for P.I 3. Usage of technical solution for P.I
	Cyber deviation	1. Education & Awareness for preventing cyber deviation 2. Establish counter measure for cyber deviation (compliance law)
Index for cyber Threat Experience (7 indicators)	Information security	1. # of zombie PC detection 2. # of website hacking detection
	Personal information security	1. # of report on P.I infringement 2. # of website exposing P.I
	Cyber deviation	1. Incidence of cyber crime 2. Ratio of internet addiction 3. Ratio of malicious reply on major website
Index or cyber threat Sensory level (3 indicators)	Information security	1. Awareness on cyber threat 2. (Do they know cyber threat?) 3. possibility of cyber threat 4. (Do they think cyber threat could happen?) 5. Seriousness of damage by cyber threat (how serious do they think about damage?)
	Personal information security	
	Cyber deviation	

Chỉ số ATTT số Việt nam (thử nghiệm)

- Dựa trên kết quả khảo sát với 45 câu hỏi
- Tính điểm từ 1-100, trong đó gần 100 có

Kết quả
Chỉ số ATTT số 2012 là 26%

  - o Mức độ xảy ra sự cố thấp nhất có thể
  - o Mức độ cảnh giác về mất ATTT cao nhất
- Tập trung vào 23 indicators, có trọng số từ 1-3

VNISA

VIETNAM INFORMATION SECURITY ASSOCIATION

Chung tay xây dựng Hạ tầng thông tin an toàn vì Chủ quyền số Quốc gia

Together build Secure Information Infrastructure for National Digital Sovereignty

Xin chân thành cảm ơn