



SACRAMENTO STATE
Redefine the Possible

Cyber Security In Public Institutions

Larry Gilbert, Vice-President & CIO
Fall 2015

Sacramento State Quick Facts and Figures

- 30,000+ students
- ~5,000 staff
- 300,000+ alumni
- 30,000 applicants
- Many more affiliated ‘persons of interest’

Information Security At Sacramento State

- Basis is California Information Security Act of 1977
- CSU information security overseen by Board of Trustees and its Audit Committee
- There is a comprehensive CSU information security policy
- Campus information security is the president's responsibility
- Risk can only be delegated to the Chief Information Officer and/or an Information Security Officer

Mass Malware of the Past

[SPAM]ATM International Credit Settlement,

Central Bank of Nigeria. [printer@brandmellon.co.uk]

Sent: Sat 10/13/2012 5:20 AM

To: dave@d

Central Bank of Nigeria.
ATM International Credit Settlement,
Directorate of International Payment.

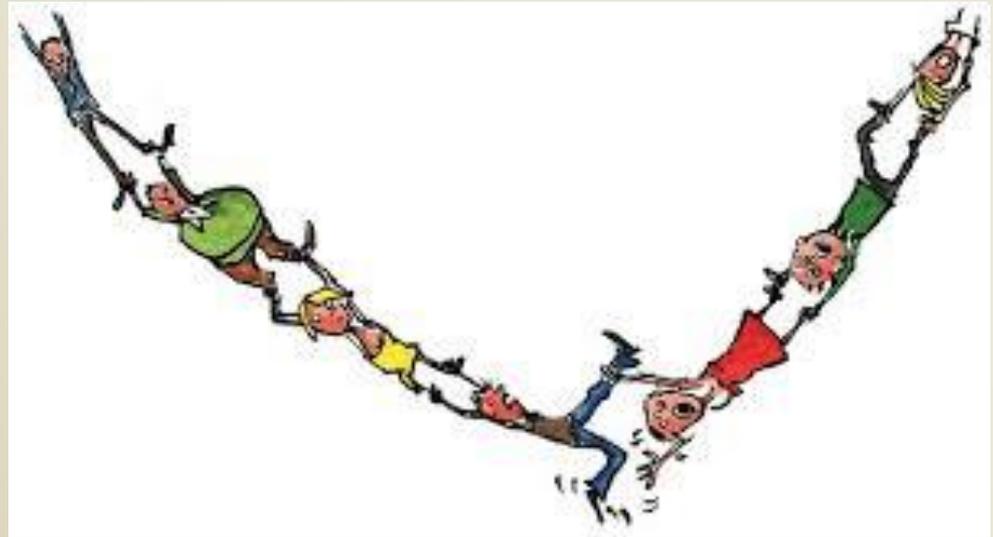
This is to officially notify you about your Fund that was supposed to be rendered to you via numerous ways i.e. Courier Companies, Western Union Money Transfers and Banks. Due to this lost of Funds of yours which was suppose to be given to you but failed to. So in this case, a beneficial meeting was held on the 25th of August 2012 at the World Bank in Switzerland, which top officials and Central Bank Governors from different countries in the world were present at the meeting. Which they discussed on how your Fund can be given to you without any loss at this time, which you have to stop any further communication with any other person(s) or office(s) to avoid any hitches in receiving your ATM payment.

In conclusion at the meeting, The President of World Bank Mr. Jim Yong Kim has strictly authorized 6 Banks in the World to deliver all Funds through courier companies. Your Fund which is truly \$3.5 Million USD (Three Million, Five Hundred Thousand United States of America Dollars) to all beneficiaries in various countries in the world as an ATM MASTER CARD. Below are the authorized Banks;

Daiwa Bank R/Osaka/Japan.
Caja De Madrid/Madrid/Spain.
Lloyds Bank R /London/England.
Central Bank of Nigeria/Lagos/Nigeria.
Banco di Santo Spirito/Rome/Italy.
Bank of New York Mellon Corp/New York/USA.

Each of this Banks are to distribute 150 ATM MASTER CARDS to every beneficiaries in the World that are to receive their compensation ATM CARD, so this Bank (Central Bank Of Nigeria) will send you your ATM CARD which you will use to withdraw your money in any ATM machine in any part of the world, but the maximum withdrawal is \$50,000 US dollar per day. Note that this ATM CARD of yours has been activated and a security pin code number will be issued to you from this Bank as soon as you receive your Card for a safer withdrawal. Please contacts the ATM CARD payment departments Mr. Khalid Anderson information are as below;

Weakest Link Principle



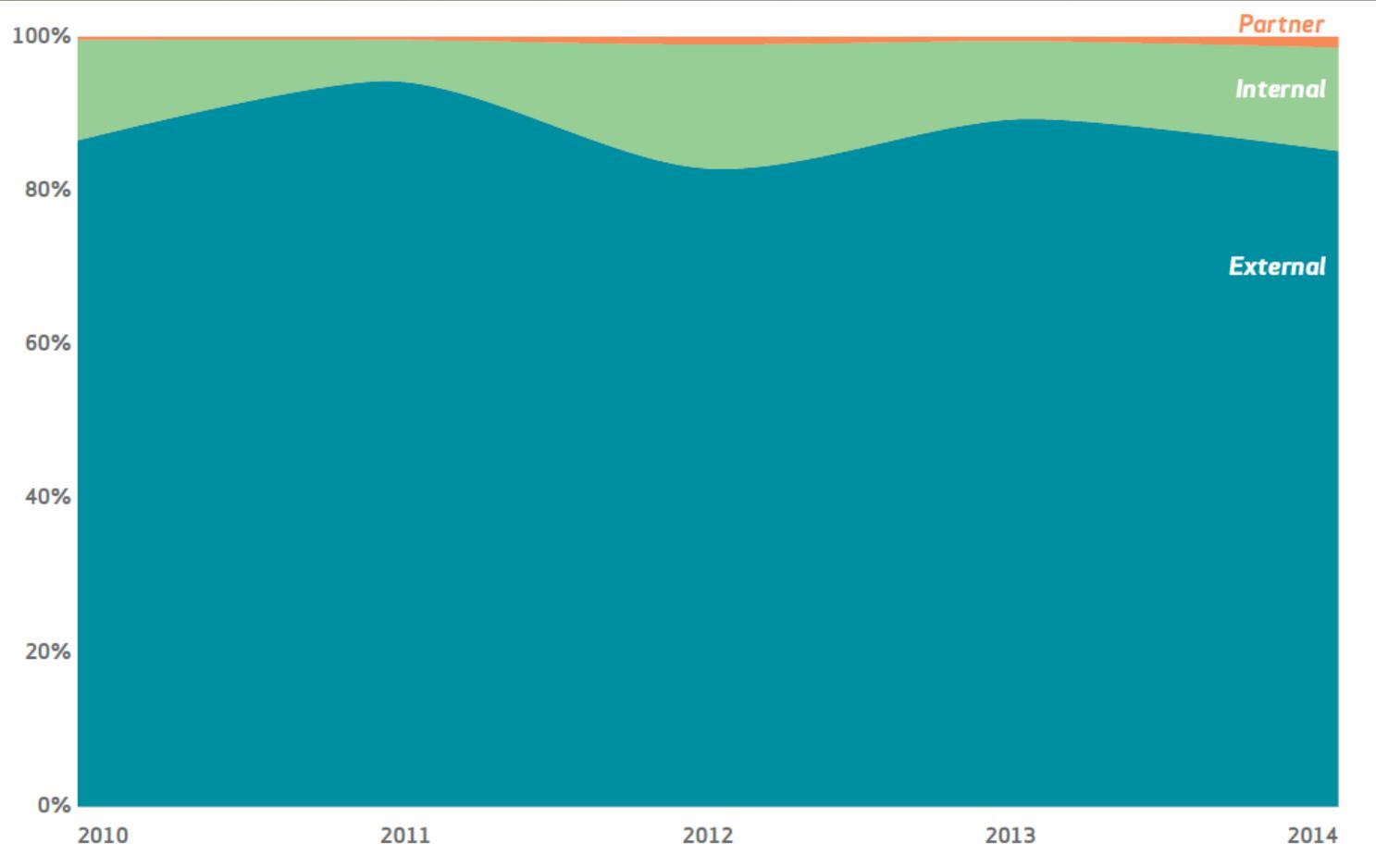
05 Target Hackers Broke in Via HVAC Company

FEB 14

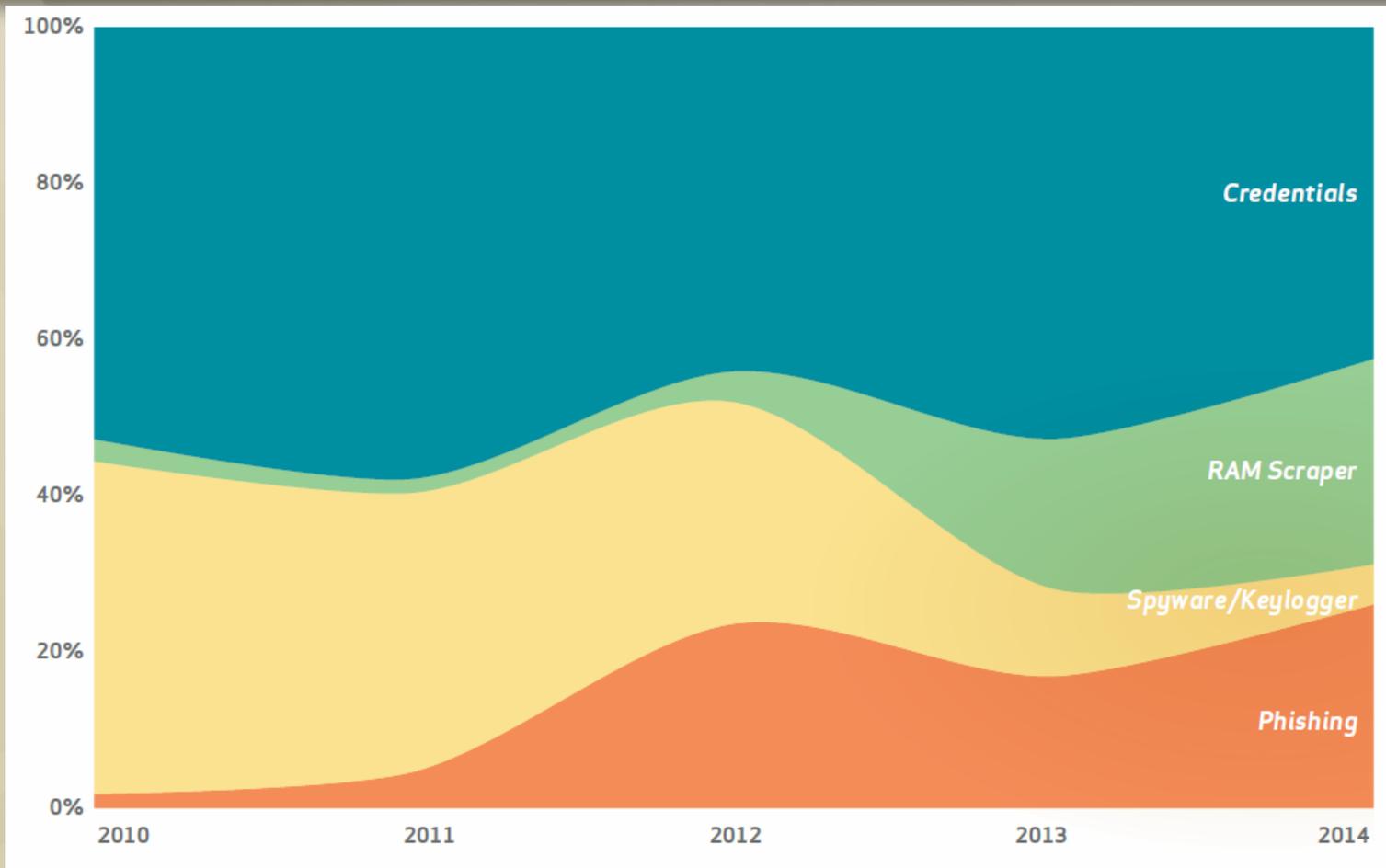


Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

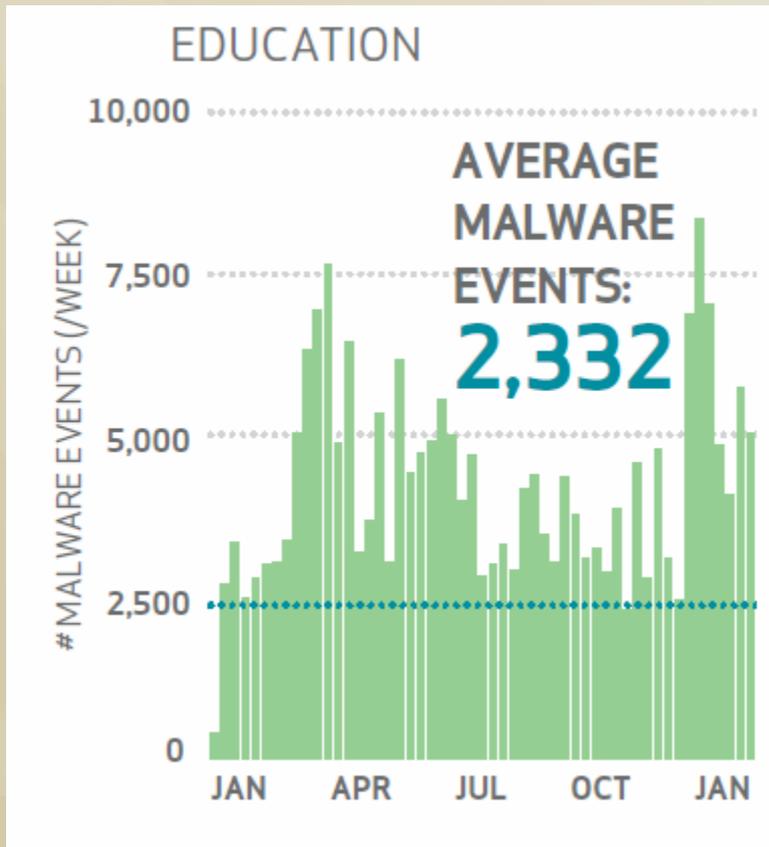
Where Do Attacks Originate?



Key Threat Actions Over Time



Isn't A Lot of Malware The Same?

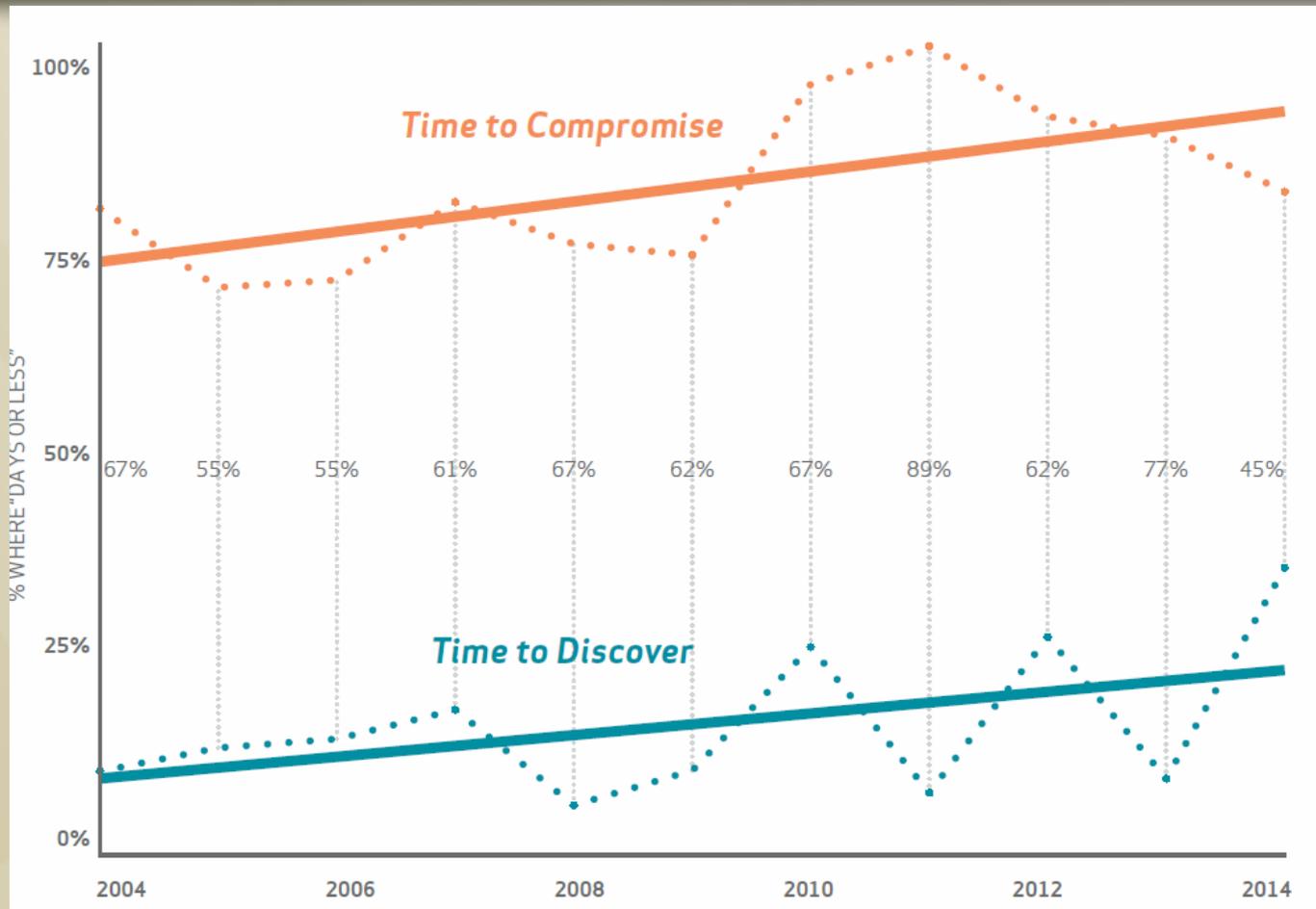


70-90%

OF MALWARE SAMPLES
ARE UNIQUE TO AN
ORGANIZATION.



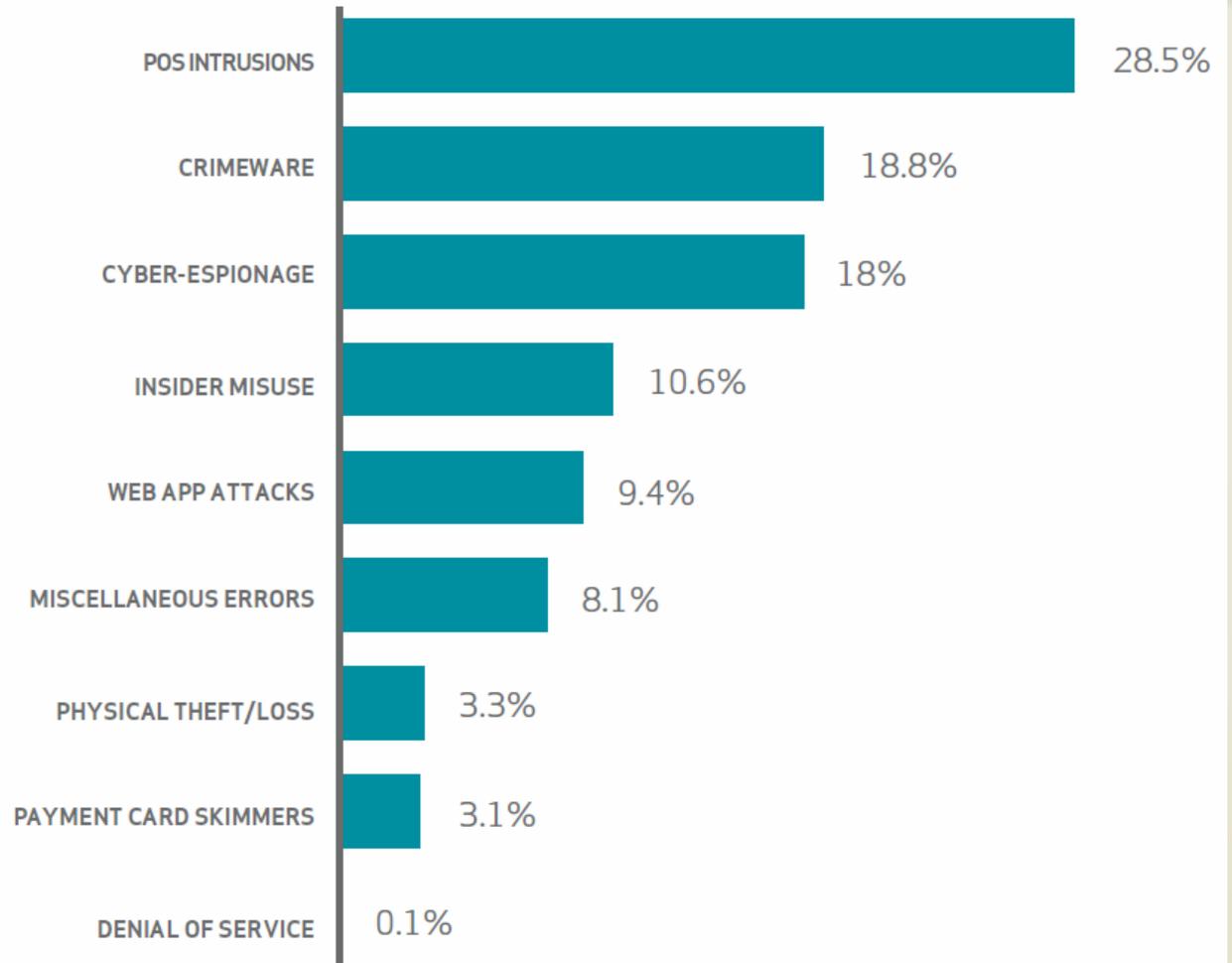
The Hackers Don't Need Much Time



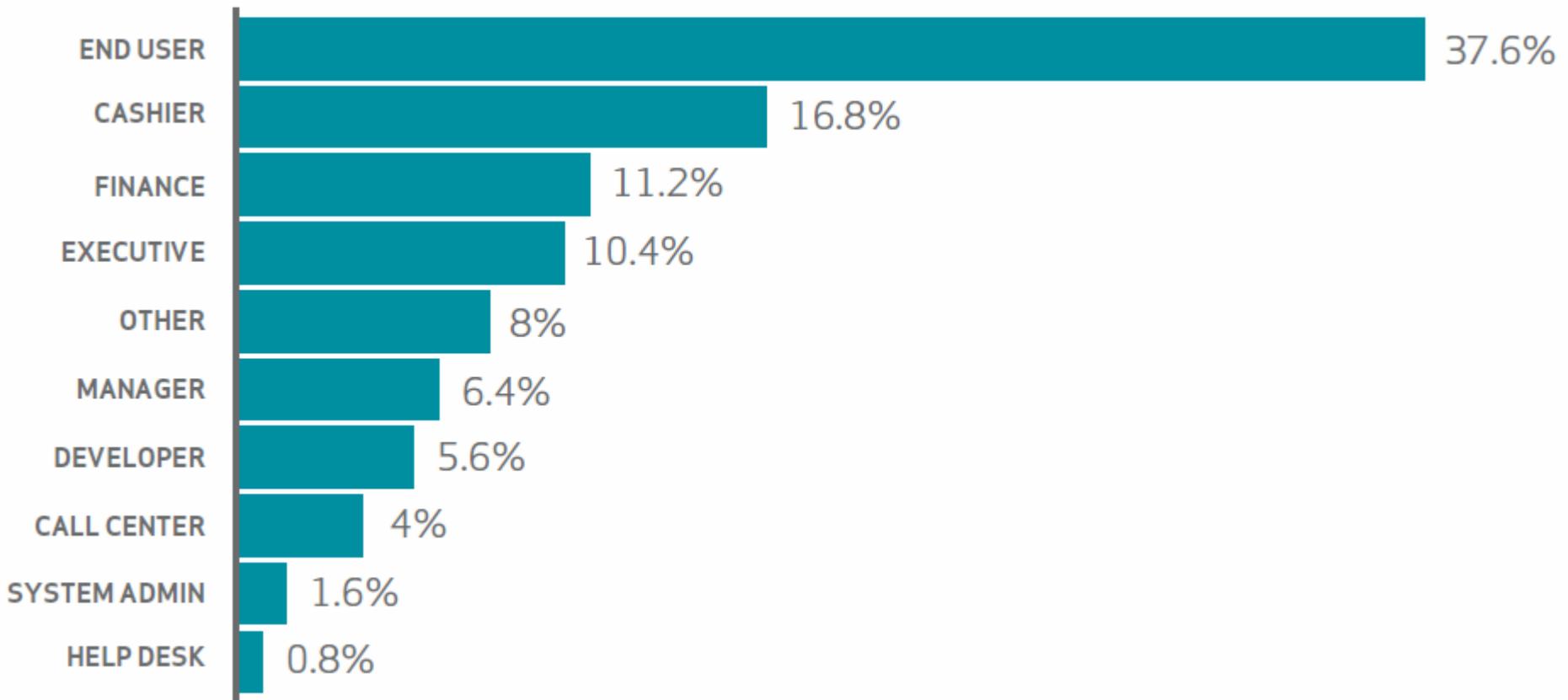
The Intent Is Usually To Spread
the Threat - Quickly

75% of attacks spread from
Victim 0 to Victim 1 within
one day (24 hours)

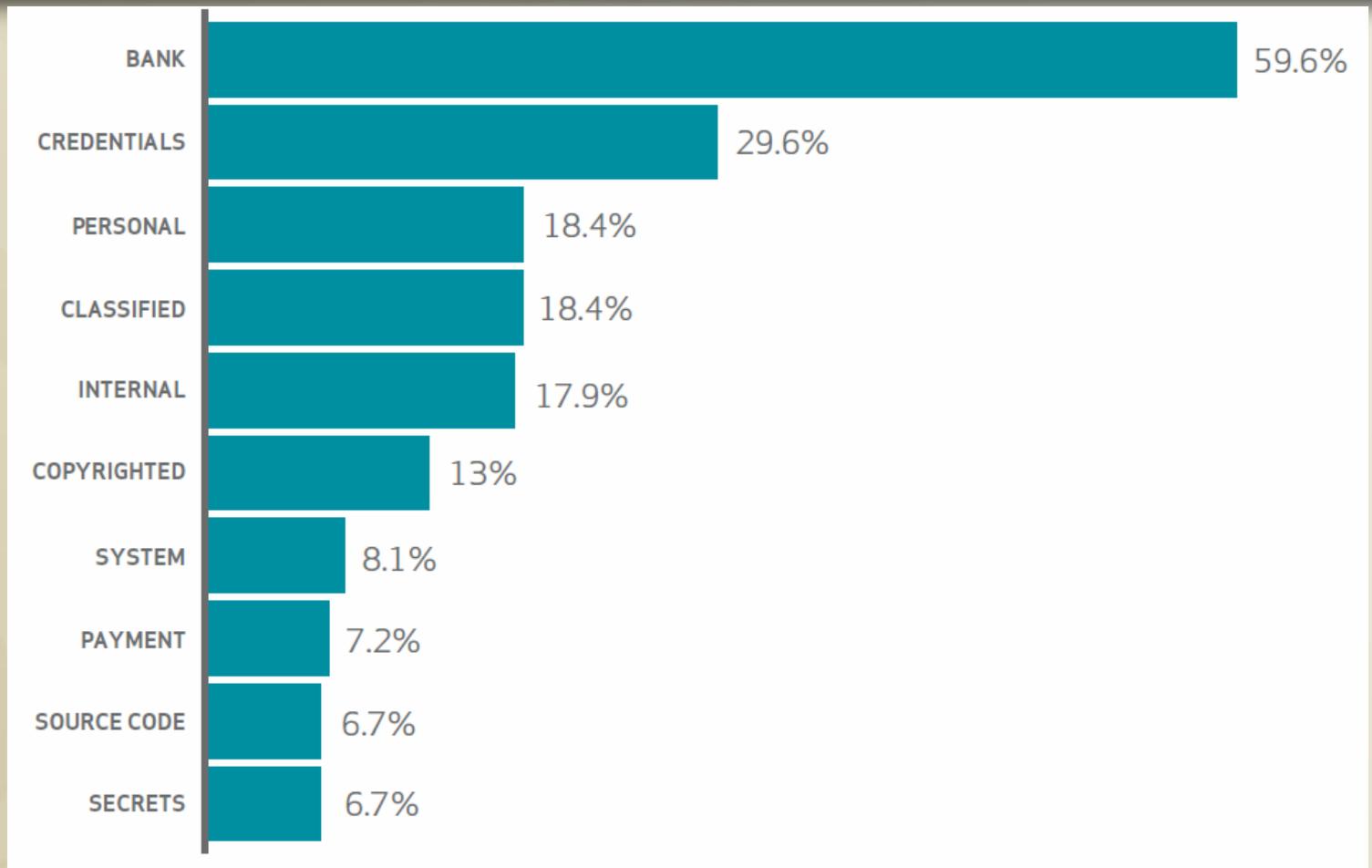
People As Common Denominator



And It's Not Just Systems Administrators



Purpose of Crimeware Attacks: Credentials and Money



Stolen Credentials Used To Log Into Web Apps

95%

OF THESE INCIDENTS
INVOLVE HARVESTING
CREDENTIALS STOLEN
FROM CUSTOMER
DEVICES, THEN
LOGGING INTO WEB
APPLICATIONS
WITH THEM.



Phishing Is A Key Technique

BEIJING STAR TAK FUNG BO CULTURE MEDIA LTD.

September 9, 2015

Attn:
Robert S. Nelsen
Crystal Springs Uplands School

INVOICE

651-243-1817
eddie@kcdottthan.com

Invoice Payment Needed

Sum of Payment \$100,000.00

Total \$100,000.00

We would appreciate you having your account department wire funds to the following

Wire Instruction for Payment Below

COMPANY NAME: Beijing Star Tak Fung Bo culture media Ltd.
COMPANY ADDRESS: Jianguo Road, Chaoyang District, Beijing No. 88 SOHO New Town,
Block B
BANK NAME: China Construction Bank
BANK ADDRESS: Shijingshan Road, Shijingshan District, Beijing, China Construction Bank
Building, on the 22nd floor
SWIFT CODE: PCBCCNBJBJX
A / C No : 955-330-011-032-832



Phishing Is Difficult Or Impossible To Trace

Received: from smtprelay.b.hostedemail.com (64.98.42.205)

```
NetRange: 64.98.0.0 - 64.98.255.255
CIDR: 64.98.0.0/15
NetName: TUCOWS-BLK2
NetHandle: NET-64-98-0-0-1
Parent: NET64 (NET-64-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS394308, AS15348, AS32490
Organization: Tucows.com Co. (TUCOW)
RegDate: 2000-05-18
Updated: 2015-08-06
Ref: http://whois.arin.net/rest/net/NET-64-98-0-0-1
```

```
OrgName: Tucows.com Co.
OrgId: TUCOW
Address: 96 Howat Avenue
City: Toronto
StateProv: ON
PostalCode: M6K-3M1
Country: CA
```

64.98.42.205 geolocates to Toronto ON Canada

```
Domain Name: CSUSEDU.COM
Registry Domain ID: 1958766852_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-09-09T18:29:11Z
Creation Date: 2015-09-09T18:29:11Z
Registrar Registration Expiration Date: 2016-09-09T18:29:11Z
Registrar: TUCOWS, INC.
```

Accounts Payable SpearPhishing

- Researched cash handling
- Broke credentials of one person
- Social engineered and dug deep into account
- Compromised key bank credentials
- Only saved by change of bank and two-factor authentication

Executive SpearPhishing Far More Common

The screenshot displays an email conversation. The first message is from Robert S. Nelsen (robertnelsen@csusedu.com) titled "Invoice Payment", dated Wednesday, 9/9/2015 at 11:38 AM. It is addressed to Lee, Ming-Tung. A reply from Lee, Ming-Tung is shown below, dated 9/9/2015 at 11:42 AM, with the text "Mike, Are you in the office at the moment?". The second message is another from Robert S. Nelsen, titled "Re: Invoice Payment", dated Wednesday, 9/9/2015 at 11:54 AM. It is addressed to Lee, Ming-Tung. A reply from Lee, Ming-Tung is shown below, dated 9/9/2015 at 12:00 PM, with the text "Robert". The main body of the second message contains the text: "Its OK, I just want to know if it is not too late to send ou an international wire transfer today. Can you find out as soon as possible? I will be attending an import ant meeting right now and i want you to get back to me as soon as you can as i arrange the instructions. waiting for your email." Below this, there is a signature "Robert" and a footer that reads "On 2015-09-09 18:42, Lee, Ming-Tung wrote:".

And They Are Persistent

www.2011.com
Robert S. Nelsen <robertnelsen@csusedu.com>
Re: Invoice Payment

To: Lee, Ming-Tung

Message: Beijing Star Talk Fung.pdf (276 KB)

See attachment for the instructions. Email me with the transfer confirmation as soon as it is done.

Robert

On 2015-09-09 19:00, Lee, Ming-Tung wrote:

Will do.
Mike

Thu 9/10/2015 10:47 AM
Robert S. Nelsen <robertnelsen@csusedu.com>
Re: Invoice Payment

To: Lee, Ming-Tung

Mike,

Any update about the international wire transfer yet? still waiting to read from you with the wire confirmation.

Robert

Phishing Is Increasingly Dangerous

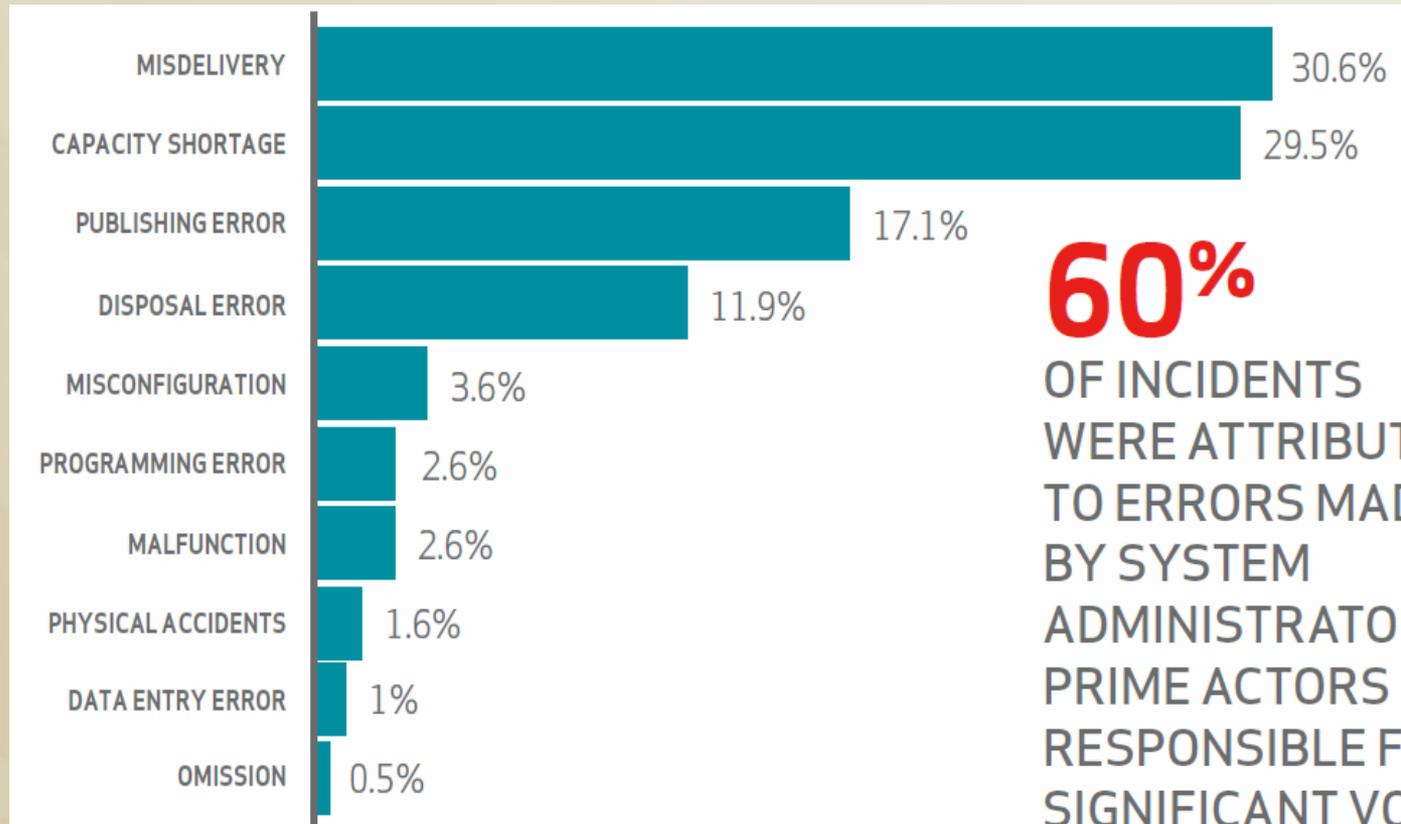
“For two years, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing. The user interaction is not about eliciting information, but for attackers to establish persistence on user devices, set up camp, and continue their stealthy march inside the network”

How Do You Combat Phishing?

"One of the most effective ways you can minimize the phishing threat is through awareness and training."

- —Lance Spitzner, Training Director,
- SANS Securing The Human

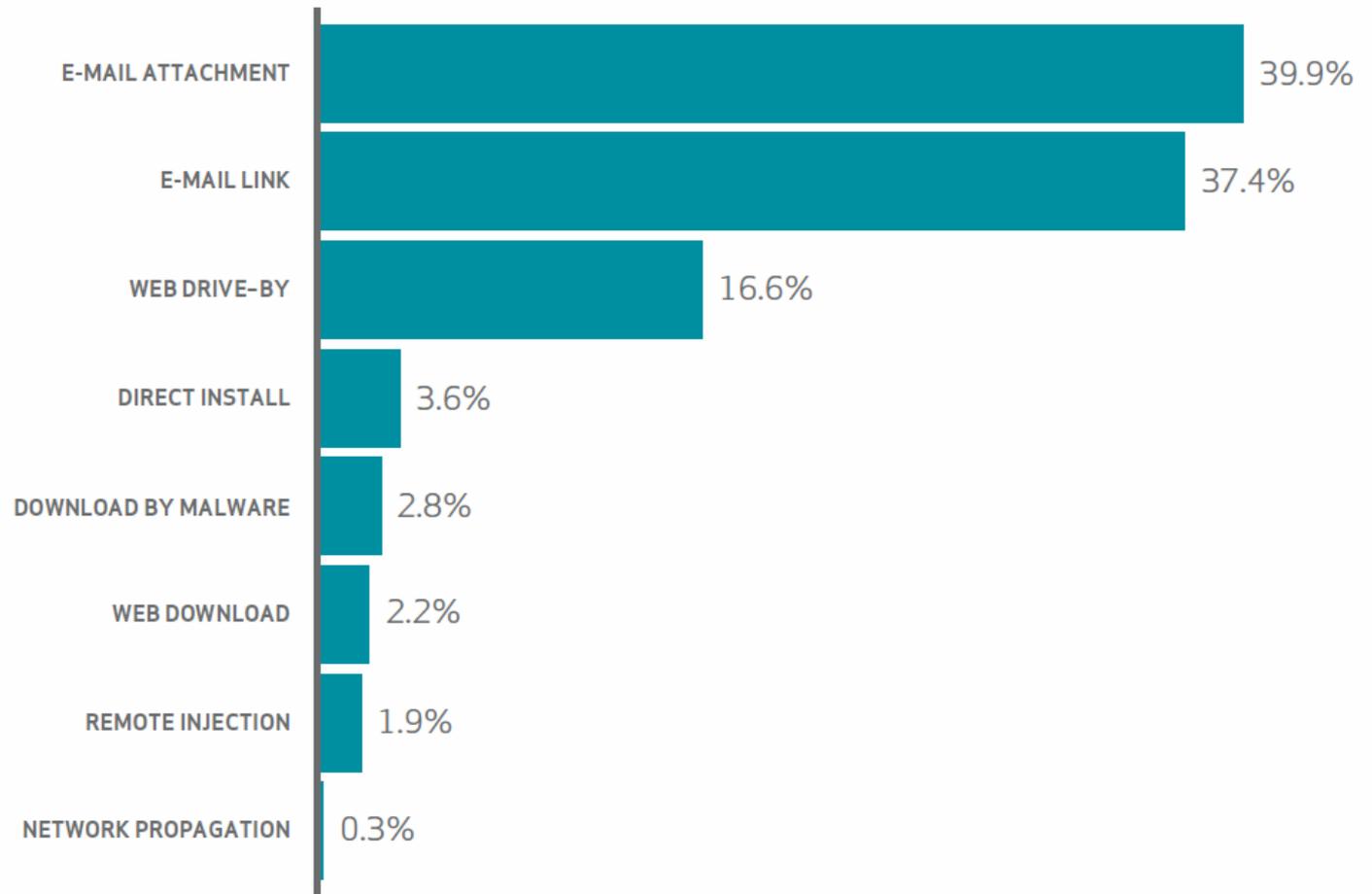
Human Error And Intentional Misuse



60%

OF INCIDENTS WERE ATTRIBUTED TO ERRORS MADE BY SYSTEM ADMINISTRATORS—PRIME ACTORS RESPONSIBLE FOR A SIGNIFICANT VOLUME OF BREACHES AND RECORDS.

Importance of Email and Web Access



Targeted Malware: Don't Click!

- Malware is often targeted at high-risk users
- Can include spoof 'official' emails, malvertising, 'account' alerts, etc.
- Need sophisticated tools like FireEye
- Sac State monitors 24 of most critical network segments on campus looking for web-based malware, phishing, an evidence of malware exfiltration
- We filter 1 Gb of 2-3 Gb of incoming traffic

What Can We Do?

- Awareness is key
- Apply appropriate resources consistently
- Monitor logs, email, and behavior
- Lock down high-risk information and functions
- Share - MSISAAC

Let's discuss