ControlCase
Compliance as a Service

Compliance Through Security

Jeff Wilder CISSP,ISSAP,ISSMP,CISA,CGEIT
PCI Security Standards Council

Question?

If you found out that you were going to be breached tomorrow, would you do anything different?

If there are, why are you not doing them today?

ControlCase
Compliance as a Service

Information Security is Complicated

ControlCase
Compliance as a Service

Verizon Breach Report Statistics

2014 & 2015 Data

ControlCase
Compliance as a Service

No one is immune from attack or breach

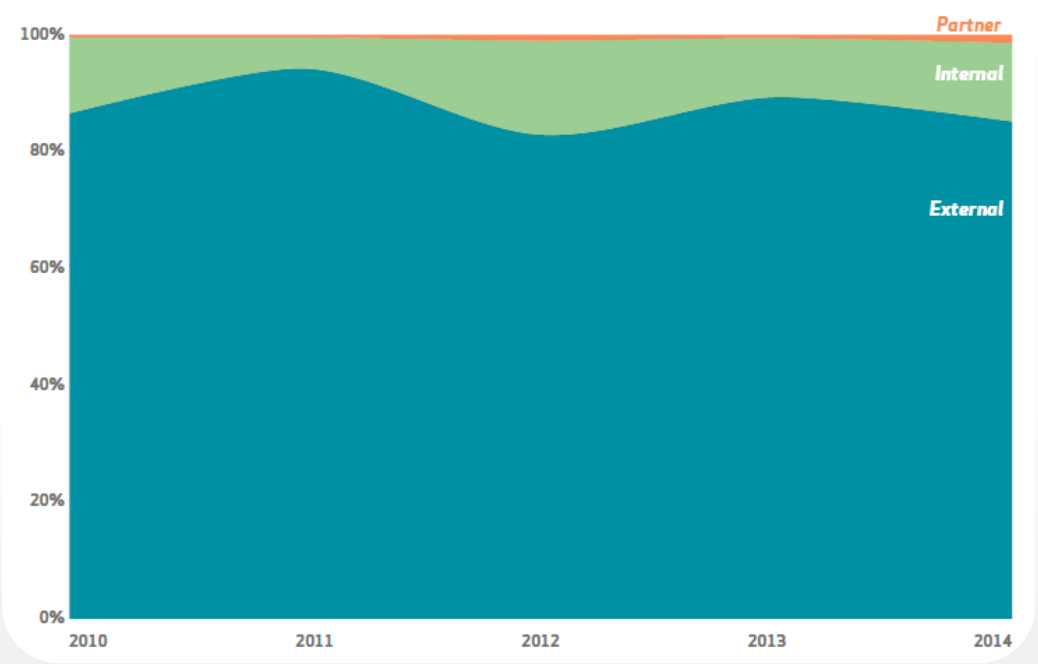
	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

(Verizon 2015 Data Breach Investigation Report 3)

ControlCase
Compliance as a Service

Threat vectors

Who is getting to your data?



3% Partner

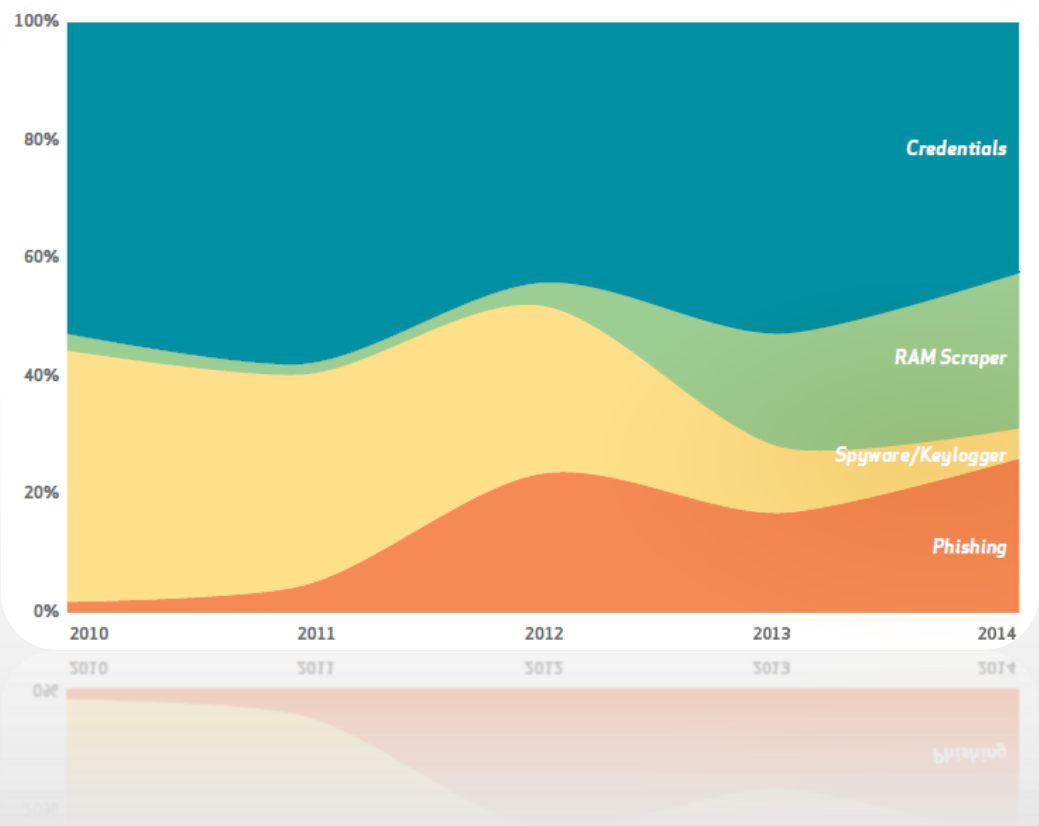
12% Internal

85% External

(Verizon 2015 Data Breach Investigation Report 4)

ControlCase
Compliance as a Service

Attack Vectors



How are they getting the data?

- **Compromised Credentials**
- **Ram Scrapers**
- **Key Loggers**
- **Phishing Attack**

(Verizon 2015 Data Breach Investigation Report 5)

ControlCase
Compliance as a Service

Is it really that easy?

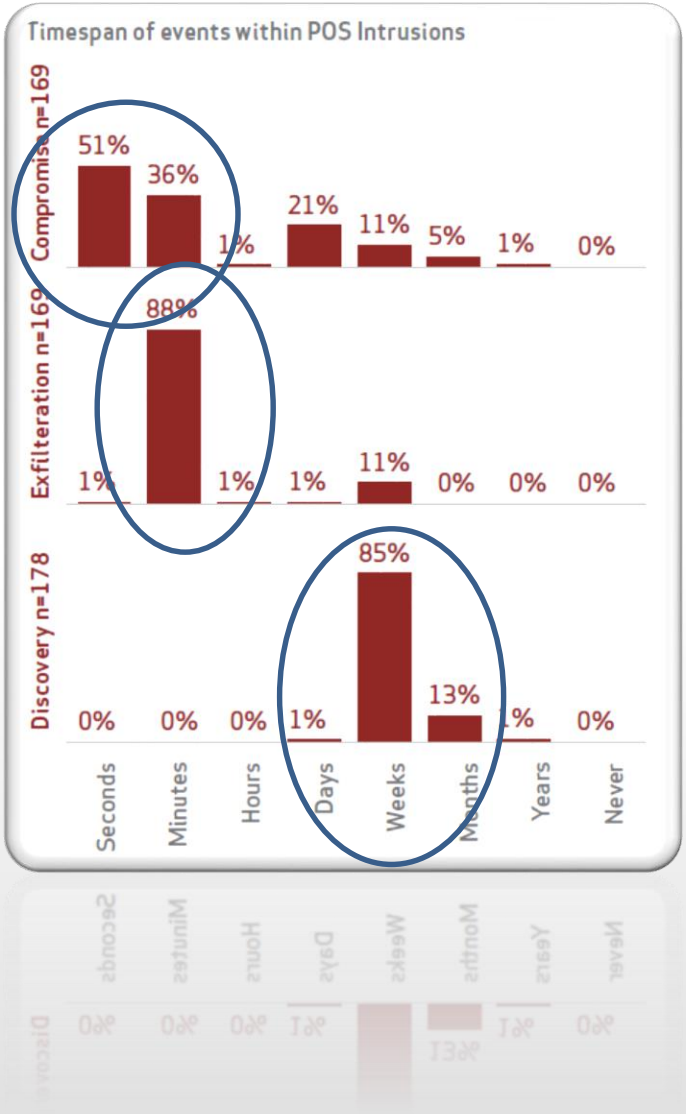
- "About half of the CVEs exploited in 2014 went from publish to pwn in less than a month."

- "We found that 99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published."

(Verizon 2015 Data Breach Investigation Report 11)

ControlCase
Compliance as a Service

Once they are in?



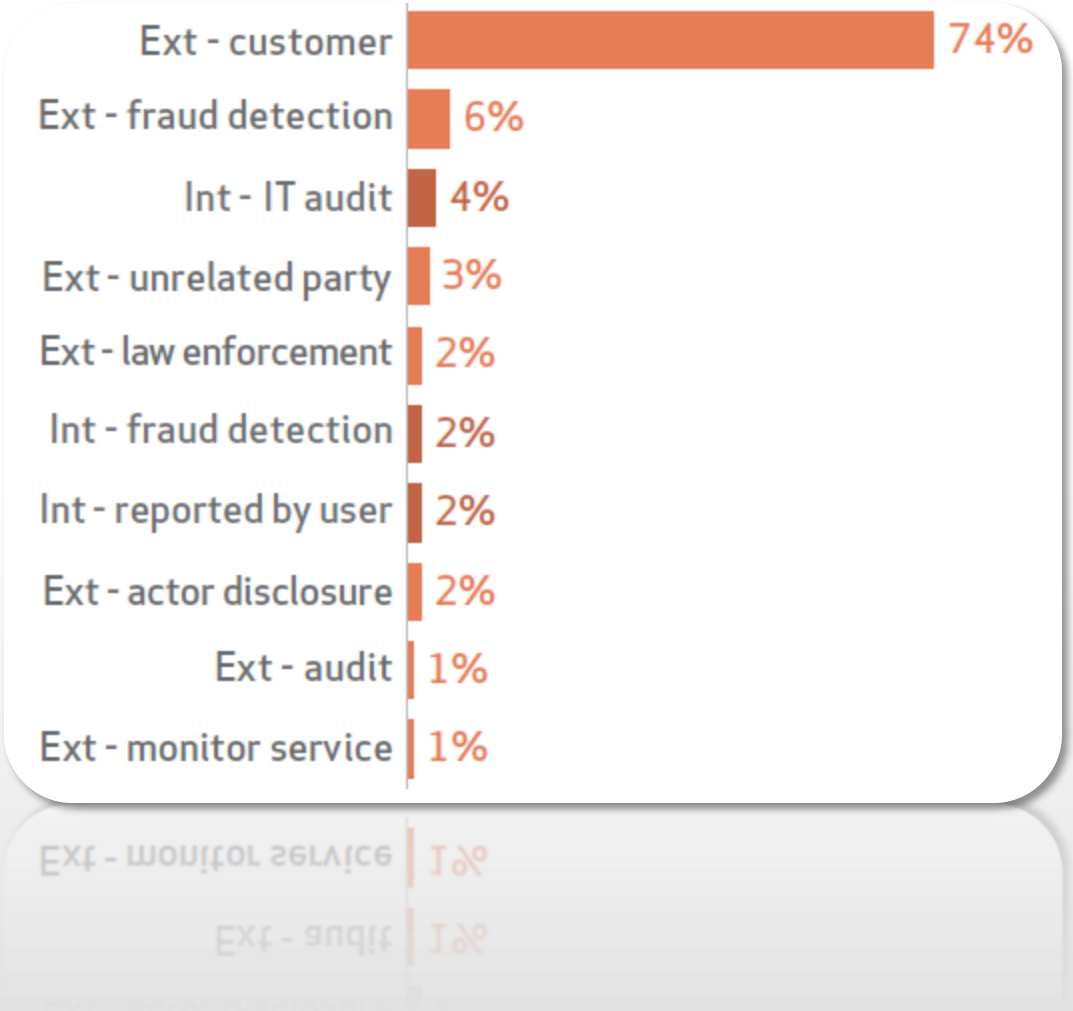
Chilling Statistics:

- **87% of the POS systems were compromised in less than an hour**
- **89% of the compromised POS systems had data exfiltrated in less than an hour after compromise**
- **86% of the compromised POS systems were discovered in less than a month**

(Verizon 2014 Data Breach Investigation Report 16)

ControlCase
Compliance as a Service

How is the breach discovered?



" 99% of the notifications were external parties (primarily CSIRTs) contacting victims to let them know their hosts were involved in other attacks"

(Verizon 2014 Data Breach Investigation Report 21)

Big data breaches 2014

- Neiman Marcus
- White Lodging
- Sally Beauty
- Michaels
- 11 casinos
- New York
- PF Changs
- Albertsons & SuperValu
- Community Health Systems
- UPS
- Dairy Queen
- Goodwill
- Home Depot
- Jimmy John's
- JP Morgan Chase
- Sourcebooks
- Kmart
- Staples
- Bebe
- Sony

The Big Data Breaches of 2014, Forbs

ControlCase
Compliance as a Service

Compliance vs. Security

ControlCase
Compliance as a Service

Compliance vs. Security

Compliance does not make you secure

Compliance - The act or process of doing what you have been asked or ordered to do

Security - The state of being protected or safe from harm

"Compliance is asking you to put a lock on the door. Security is making sure you lock it every day."(Bob Russo)

Merriam-Webster

ControlCase
Compliance as a Service

Becoming Secure

So how do we get from compliance to security

- Many of the security frameworks do not include controls around:
  - Governance and Oversight
  - Metrics and Reporting

- Security frameworks are generally a *one-size-fits-most* and do not account for your:
  - Individual business drivers
  - Organizational size
  - Complexity

ControlCase
Compliance as a Service

Are you a good gardener?

Becoming Secure

Governance and Oversight

- Are your controls truly effective?
- How do you ensure their ongoing continuity?
- Do you have executive oversight?

Going above and beyond

Are your controls truly effective and address the RISK?

- Anti-malware
- Authentication
- Vulnerability identification

Going above and beyond Compliance

How do you ensure their ongoing continuity?

- Can you affirm with 100% certainty that you are secure this very moment?

Going above and beyond Compliance

Do you have executive oversight?

- What is your company's strategic plan for security?
- To whom does your security team report to?
- Do you have the right people and business partners to help?
- What about vendor management?
- How are the resources for security allocated?
- Is your spend today a good value and provide benefit tomorrow?

ControlCase
Compliance as a Service

Closing Thoughts and Considerations

1. If you don't need it, get rid of it
2. Devalue the data
3. Invest in good people
4. Implement a robust training program
5. Be proactive
6. Find a good business partner to help and provide you guidance
7. Acquire the right tools
8. Information share with organizations within your same vertical
9. There are limitations in doing what needs to be done vs what should be done.

ControlCase
Compliance as a Service

Things To Take Away

- Being complaint does not ensure that you are secure
- Focus on truly being secure, compliance will follow
- Security is not an event, Is not an end state- it's a process

Questions?

Work Cited

Merriam-Webster. Merriam-Webster, n.d. Web. 13 Oct. 2015.

"The Big Data Breaches of 2014." *Forbes*. Forbes Magazine, 13 Jan. 2015. Web. 13 Oct. 2015.

Verizon 2015 Data Breach Investigation Report. Rep. 2015 ed. Virginia: Verizon, 2015. Print

ControlCase
Compliance as a Service