SecureWorld
Web Conference – *Incident Response: Clean Up on Aisle Nine*

Sponsored by:

November 29, 2012
10 AM PST
Moderator

Bryan Cline, PhD

VP, CSF Development & Implementation, CISO Health Information Trust Alliance (HITRUST)
Web Conference Agenda

Cédric Laurant, Esq.  
Attorney  
Cédric Laurant Law Firm & Ulys

David Matthews  
Director of Incident Response  
Expedia, Inc.

James Colby  
Vice President  
Radware
Data Breaches & the Upcoming Data Protection Legal Framework: What’s the Buzz in Europe? What U.S. Companies Should Know

Cédric Laurant, Esq.  
Attorney, Cedric Laurant Law Firm & Ulys (Brussels)
DATA BREACHES AND THE UPCOMING DATA PROTECTION LEGAL FRAMEWORK: WHAT’S THE BUZZ IN EUROPE? WHAT US COMPANIES SHOULD KNOW

SECUREWORLD WEB CONFERENCE:
“INCIDENT RESPONSE: CLEAN UP ON AISLE NINE”

NOVEMBER 29, 2012

Cédric Laurant
Attorney-at-Law, Cabinet Ulys (Brussels)
Owner, Cedric Laurant Law Firm

www.ulys.net - www.droit-technologie.org
As the upcoming EU privacy framework is in the spotlight these days in Brussels, US companies must realize that the new rules will impact their data privacy and information governance obligations, whether they are present in Europe or not.
From 2015, the European data protection legal framework will change substantially in various ways. What is relevant to know in the context of this web conference is: the scope of application (the rules will apply to US companies even if they are not located in the EU), and the extent of the data security and data breach notification measures.
WHAT’S IN THIS PRESENTATION FOR ME?

You’ll learn about:

- A) whether your company has to care about those rules now, in the short, medium or long term.
- B) what is likely to change from the current regime.
- C) the cases in which the data breach notification and data security requirements are different than the ones in the United States and how it is going to change with the revision of the data protection legal framework.
- D) whether your company should change some of its procedures or policies in place to tackle the new data breach notification requirements.
- E) some of the solutions that can help your company to be ready for the compliance challenge of the new DP Regulation.
- F) essential take aways.
A) DOES YOUR COMPANY HAVE TO CARE ABOUT THOSE RULES NOW, IN THE SHORT, MEDIUM OR LONG TERM?
A) DOES YOUR COMPANY HAVE TO CARE ABOUT THOSE RULES NOW, IN THE SHORT, MEDIUM OR LONG TERM?

In the short term
IN THE SHORT TERM

- i. if your company is a provider of publicly available electronic communications services (telecom company, ISP): notification of data breaches mandatory since June 2011 (check national law of EU Member State where your company is based).

- ii. if your company is not a provider of publicly available electronic communications services but does business in EU Member State where a law already compels notification of data breaches to all data controllers, regardless of the sector they belong to. As of now, it is still the exception (only a few countries have such laws), until the new DP Regulation enters into force (2015).
iii. if your company is not a provider of publicly available electronic communications services, does business in a EU Member State, but in a Member State where a data breach notification law has not been enacted yet, there is still a possibility to be subject to mandatory notification based on whether the interpretation of the country’s general data protection law or regulations, or a strict DPA’s guidelines, mandates or recommends a notification. As of now, it is the case in about 10-15 countries.
A) DOES YOUR COMPANY HAVE TO CARE ABOUT THOSE RULES NOW, IN THE SHORT, MEDIUM OR LONG TERM?

In the medium term
IN THE MEDIUM TERM

i. the upcoming Data Protection Regulation is scheduled to enter into force around 2015. No delay for implementation by Member States since it is a Regulation.

ii. high impact of a notification to the public because of potential media backlash and impact on reputation on the US subsidiary based in Europe but also on the company based in the US.
A) DOES YOUR COMPANY HAVE TO CARE ABOUT THOSE RULES NOW, IN THE SHORT, MEDIUM OR LONG TERM?

In the medium to long term (3-5 years)
IN THE MEDIUM TO LONG TERM (3-5 YEARS)

- Implementing and delegated acts further specifying the conditions and requirements of the notification of data breaches: may take some time to get drafted by the Commission and expert groups. In the meantime, there is uncertainty due to the lack of Data Protection Authorities’s guidelines on the issue or, if they exist, about which ones will apply in which circumstances.
B) WHAT ARE THE GENERAL CHANGES THAT ARE LIKELY TO TAKE PLACE BETWEEN THE CURRENT AND UPCOMING DATA PROTECTION LEGAL REGIME?
B) WHAT ARE THE GENERAL CHANGES THAT ARE LIKELY TO TAKE PLACE BETWEEN THE CURRENT AND UPCOMING DATA PROTECTION LEGAL REGIME?

- a. Data Protection Regulation:
  - is still being discussed ⇒ some provisions may still change substantially.
  - Likely timeline of legislative process of the Regulation.
B) WHAT ARE THE GENERAL CHANGES THAT ARE LIKELY TO TAKE PLACE BETWEEN THE CURRENT AND UPCOMING DATA PROTECTION LEGAL REGIME?

b. Current regime:

i. Scope of application of the General Data Protection Directive (95/46/EC) and updated e-Privacy Directive (2002/58/EC modified by 2009/136/EC) to data controllers. Avoid misconception: Directive applies not only to EU citizens or EU residents but also to the personal data of non-Europeans whose data is processed in the EU and to companies with HQ or suppliers in Europe.

ii. Data subject’s right of access: unlike in the US, right is generally more extensive and enables data subject to obtain more information and object to processing, even obtain information about logic governing processing of his personal information if a decision has been made about him automatically. ⇒ take into account when implementing a data breach notification procedure in your company.
B) WHAT ARE THE GENERAL CHANGES THAT ARE LIKELY TO TAKE PLACE BETWEEN THE CURRENT AND UPCOMING DATA PROTECTION LEGAL REGIME?

- c. Future regime:
  - i. Scope of application: any personal data processed in the EU + any personal data processed by a controller not based in the EU but whose processing activities are directed to or serve to monitor a data subject residing in the EU;
  - ii. Right of access: controller must provide means for electronic request if processes personal data by automated means. Commission may adopt implementing acts for laying down standard forms and specifying standard procedures; also for specifying the standard forms by which controllers, sector by sector, have to provide the information to data subjects, and the procedures for requesting access (for data subjects) and granting (for controllers).
B) WHAT ARE THE GENERAL CHANGES THAT ARE LIKELY TO TAKE PLACE BETWEEN THE CURRENT AND UPCOMING DATA PROTECTION LEGAL REGIME?

- c. Future regime:
  - iii. Right to be forgotten and to erasure, right to data portability and right to object to processing: consequences on the management of data breaches.
  - iv. Requirement to hire a DPO: role; can be outsourced for SMEs, must be hired internally in the case of companies with more than 250 employees but criterion may change); sanctions will be higher for violations of the DP Reg.;
  - v. Collective redress mechanisms: consequences on the implementation and management of data security measures.
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

SHORT-TERM PERSPECTIVE: what should your company under the current framework (General Data Protection Directive and e-Privacy Directive)?
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

**Hypothesis:** your company is facing a data breach that has EU elements (personal data of individuals living in the EU or subsidiary is located in one or several EU Member States) and wishes to know what are its obligations under the laws of those EU Member States.

**Issue:** whether the law of that EU Member State requires the notification of the breach to go beyond the requirements that your company is already following with its notification under US rules.
Legal analysis:

1. Scope of application: Is it likely that the Member States’ data breach notification legal requirements will apply?
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

Legal analysis:

2. Does that jurisdiction require more than the notification your company has made to the competent authority in the US or to its customers in the United States? It depends on the type of notification involved since some EU Member States currently have different requirements depending on the type of notification involved.

- Notification to affected customers: one example: if your company did business – or most of it – in Austria, your company would not have to notify customers either in case the data breach only results in non-economic damage, or the potential damage is minor, or the cost of informing all customers would be disproportionate, which must be assessed against the potential damage the breach may cause. Unless you became aware of a “systematic or material misuse of data” that “may cause damage to the data subject”.

- Notification to the Data Protection Authority: In Ireland, the DPA is applying an extensive “Personal Data Security Breach Code of Practice” that requires that it be notified of any unauthorized disclosure of personal data.
Legal analysis:

3. Need to make a risk assessment regarding the potential sanctions for non-compliance in the various EU jurisdictions, some of which require a higher level of notification than the notification already prepared by your company.

- Example: Spain has one of the most stringent penalty systems in the EU. Under the Spanish Data Protection Act, fines varying between EUR900 to EUR600,000 can be imposed depending on the severity of the breach. The Spanish Criminal Code also establishes criminal offences based on the violation of secrets and breach of privacy, however criminal enforcement is not common. Decisions issuing penalties have actually ranged from EUR6,000 to EUR1,091,822.
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

- Follow-up steps your company should adopt after notifying customers or the DPA:
  - Apart from notifying the breach to its affected customers or, if required, to a data protection authority, your company should implement, if it has not done so already, technical and organizational measures that provide for adequate data security (to comply with the general security requirements of the General Data Protection Directive (Art. 17, Dir. 95/46/EC).
  - If compelled to notify the breach to a DPA under the law of a EU Member State (e.g., Ireland), your company may have to demonstrate that it took the appropriate technological protection measures for the data that were breached. If it cannot demonstrate it, the DPA of the concerned jurisdiction, may mandate your company to improve its security measures by implementing the appropriate technical and organizational measures to protect personal data against future accidental or intentional destruction or loss, unauthorized disclosure or access, and all other unlawful forms of processing.
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

☐ Follow-up steps your company should adopt after notifying customers or the DPA:

☐ As part of those security measures, there may be the obligation to keep a document called “security document”, as in the case of the Spanish legislation.

- If your company has customers based in Spain, it will have to document the breach pursuant to the recommendations of the Spanish legislation. Spanish law set out a procedure for management of data breaches, including: i. establishing an internal registry (called “Security Document”) to record the type of incident and the time it occurred or was detected; ii. the effects of the breach; iii. the corrective measures applied; and iv. a record of the individuals notified (if the organization chooses to notify individuals). In practice, the level of information that must be recorded depends on the nature of the personal data concerned. The Spanish DPA is entitled to request to see the Security Document at any time. (Furthermore, Police Forces and Public Offices usually immediately report to the DPA any data breach or loss of personal data that they may be informed about (e.g. when a claim is filed with them).)
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

- Follow-up steps your company should adopt after notifying customers or the DPA:
  - Depending on the national law applicable, your company should also inform the other institutions that might be affected by the breach (e.g., banks).
C) IN WHICH CASES ARE THE REQUIREMENTS DIFFERENT THAN THE ONES IN THE UNITED STATES? HOW IS IT GOING TO CHANGE WITH THE NEW EU DATA PROTECTION REGULATION?

MEDIUM-TERM PERSPECTIVE (from 2015): Under the upcoming framework of the EU Data Protection Regulation
MEDIUM-TERM PERSPECTIVE (FROM 2015): UNDER THE UPCOMING FRAMEWORK OF THE EU DATA PROTECTION REGULATION

- Obligation to maintain appropriate technical and organizational security measures has been further specified (Art. 27 (v51)). Commission may issue delegated acts to further specify criteria and conditions for the security measures to take, state of the art, sector by sector, and for specific data processing situations, taking into account data protection by design and by default concepts.

- Importance of risk assessment.
MEDIUM-TERM PERSPECTIVE (FROM 2015): UNDER THE UPCOMING FRAMEWORK OF THE EU DATA PROTECTION REGULATION

- Data protection by design and by default (Art. 21A (v51)). Commission may issue delegated and implementing acts in order to specify criteria and requirements for the appropriate measures and mechanisms, e.g. privacy-by-design requirements applicable across sectors, products and services; and technical standards.

- Documentation requirements of controllers and processors (Art. 25 (v51)). Commission may issue delegated and implementing acts to specify documentation requirements further and establish standard forms.
General obligation of notification of a personal data breach:

- Breach of personal data.
- To the DPA (Art. 28 (v51)):
  - “without undue delay”, “not later than 24 hours after the breach has been established.
  - Contents of notification: in addition to classical requirements under the most common US state data breach notification requirements: communication of the company’s DPO or contact point; measures recommended to mitigate possible adverse effects of the breach; consequences of the breach.
  - Obligation to document all breaches.
  - Commission may issue delegated acts to further specify requirements for establishing the breach and the circumstance sin which a controller and processor is required to notify the breach, and implementing acts to specify standard format of the notification, procedures, form and modalities of the documentation requirements.
MEDIUM-TERM PERSPECTIVE (FROM 2015): UNDER THE UPCOMING FRAMEWORK OF THE EU DATA PROTECTION REGULATION

General obligation of notification of a personal data breach:

To the data subject (Art. 29 (v51)):

- Criterion: “when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject”.
- “Without undue delay and, as a rule, not later than 24 hours after the breach has been established by the controller.”
- Contents of the communication: nature of breach including categories and number of data subjects concerned and categories and number of data concerned, communication of the company’s DPO or contact point; measures recommended to mitigate possible adverse effects of the breach.
MEDIUM-TERM PERSPECTIVE (FROM 2015): UNDER THE UPCOMING FRAMEWORK OF THE EU DATA PROTECTION REGULATION

General obligation of notification of a personal data breach:

- To the data subject (Art. 29 (v51)):
  - NOT required when controller has demonstrated to DPA that it has implemented “appropriate technological protection measures”; such measures must render data unintelligible to any person not authorized to access it.
  - Commission may issue delegated acts to further specify the criteria and requirements as to the circumstances in which the breach is likely to adversely affect the data subject’s personal data; and may issue implementing acts to specify the format of the communication to the data subject.
D) SHOULD YOUR COMPANY CHANGE SOME OF THE PROCEDURES OR POLICIES IT HAS IN PLACE IN ORDER TO TACKLE THE NEW DATA SECURITY AND BREACH NOTIFICATION REQUIREMENTS OF THE UPCOMING DATA PROTECTION REGULATION?
D) SHOULD YOUR COMPANY CHANGE SOME OF THE PROCEDURES OR POLICIES IT HAS IN PLACE IN ORDER TO TACKLE THE NEW DATA SECURITY AND BREACH NOTIFICATION REQUIREMENTS OF THE UPCOMING DATA PROTECTION REGULATION?

- Gradually adapt the internal documentation your company keeps about the implementation of its data security and breach notification measures to the requirements of the upcoming Data Protection Regulation.
- Think of hiring soon a Data Protection Officer if your company comes within the scope of application of the Data Protection Regulation.
- Integrate the concept “privacy by design” within the management of data security measures.
D) SHOULD YOUR COMPANY CHANGE SOME OF THE PROCEDURES OR POLICIES IT HAS IN PLACE IN ORDER TO TACKLE THE NEW DATA SECURITY AND BREACH NOTIFICATION REQUIREMENTS OF THE UPCOMING DATA PROTECTION REGULATION?

✓ Start by using the breach notification rules that are currently applicable to your company in the US in the same way to your company’s subsidiaries in the EU.

✓ In case one of your company’s subsidiary is not based in the EU but targets its products and services to EU-based consumers or clients, start applying the same breach notification rules but making sure to gradually adapt them to make them comply with the upcoming EU requirements of the Data Protection Regulation.
D) SHOULD YOUR COMPANY CHANGE SOME OF THE PROCEDURES OR POLICIES IT HAS IN PLACE IN ORDER TO TACKLE THE NEW DATA SECURITY AND BREACH NOTIFICATION REQUIREMENTS OF THE UPCOMING DATA PROTECTION REGULATION?

✓ Be ready to put in place a way for data subjects residing in the EU and whose personal data your company is processing to get a detailed access to their personal data, according to the upcoming EU requirements of the Data Protection Regulation.
E) WHAT ARE SOME OF THE SOLUTIONS THAT CAN HELP YOUR COMPANY BE READY FOR THE COMPLIANCE CHALLENGE OF THE NEW DP REGULATION?
E) WHAT ARE SOME OF THE SOLUTIONS THAT CAN HELP YOUR COMPANY BE READY FOR THE COMPLIANCE CHALLENGE OF THE NEW DP REGULATION?

- Visualization tools: data breach charts and maps.

<table>
<thead>
<tr>
<th>Country and color for that country</th>
<th>Point scale for the country color</th>
<th>Size of DPA staff:</th>
<th>Level of all DPA fines:</th>
<th>Scope of DPA authority:</th>
<th>Status of breach notification law:</th>
<th>Coverage of data breach notification law(s) or regulation(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spain</td>
<td>5-10 points: low risk, green</td>
<td>1 point = 1-10 people</td>
<td>1 point = under 10,000 euros</td>
<td>1 point = public sector only</td>
<td>1 point = nothing</td>
<td>1 point = no statute</td>
</tr>
<tr>
<td></td>
<td>11-15 points: general risk, blue</td>
<td>2 points = 11-20</td>
<td>2 points = 10,000 - 100,000 euros</td>
<td>2 points = guidelines published</td>
<td>2 points = electronic communications providers (telcos &amp; ISPs)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16-20 points: elevated risk, yellow</td>
<td>3 points = 21-30</td>
<td>3 points = 101,000 - 500,000 euros</td>
<td>3 points = draft law in progress</td>
<td>3 points = all Information society providers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21-25 points: high risk, orange</td>
<td>4 points = 31-40</td>
<td>4 points = 500,000 - 1 million</td>
<td>4 points = law passed</td>
<td>4 points = all Information society providers and other sectors such as finance or healthcare</td>
<td></td>
</tr>
<tr>
<td></td>
<td>26-25 points: severe risk, red</td>
<td>5 points = 40+</td>
<td>5 points = over 1 million</td>
<td>5 points = regulations passed</td>
<td>5 points = all data controllers</td>
<td></td>
</tr>
</tbody>
</table>
E) WHAT ARE SOME OF THE SOLUTIONS THAT CAN HELP YOUR COMPANY BE READY FOR THE COMPLIANCE CHALLENGE OF THE NEW DP REGULATION?

- Visualization tools: data breach charts and maps.
http://databreachmaps.com
## European Data Breach Notification Requirements - As of 25 January 2012

<table>
<thead>
<tr>
<th>Law or proposed law</th>
<th>Status of law</th>
<th>Does the law follow the ePrivacy Directive?</th>
<th>Enforcement authority of the law</th>
<th>Regime of the data protection regulation</th>
<th>Interpretation by the DP Board &amp; EDPS</th>
<th>Interpretation by the EU MS courts</th>
<th>Interpretation by the CJEU</th>
<th>Updates</th>
</tr>
</thead>
</table>

[http://databreachmaps.com](http://databreachmaps.com)
<table>
<thead>
<tr>
<th>Covered Data System</th>
<th>Covered Resources</th>
<th>Definition of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>All personal data</td>
<td>All identifiable data</td>
<td>Unlawful Acquisition of data</td>
</tr>
<tr>
<td>All medical records</td>
<td>All data with Data at Rest</td>
<td>Substantial Economic Loss</td>
</tr>
<tr>
<td>Social Security Numbers</td>
<td>All data with Data in Transit</td>
<td>Substantial Identity Compromise</td>
</tr>
<tr>
<td>Other</td>
<td>Other</td>
<td>Substantial Financial Loss</td>
</tr>
</tbody>
</table>

http://databreachmaps.com
E) WHAT ARE SOME OF THE SOLUTIONS THAT CAN HELP YOUR COMPANY BE READY FOR THE COMPLIANCE CHALLENGE OF THE NEW DP REGULATION?

- Hire a DPO in the European Member State where your company does most of its business or is established. That DPO does not have to be hired internally but its functions can be outsourced (e.g., to a law firm or a consulting firm).
F) OUR ESSENTIAL TAKE AWAYS
F) OUR ESSENTIAL TAKE AWAYS

1.

✓ The Data Protection Regulation will not necessarily mean less bureaucracy (examples: DPO hiring requirement, prior consultation necessary for highly sensitive data processing activities (e.g., to assess risk); administrative process may actually take longer in certain cases; need to constitute internal documentation demonstrating compliance).
F) OUR ESSENTIAL TAKE AWAYS

2.

- **Understand the future risks** related to having to notify the European public of security breaches under the upcoming Data Protection Regulation: media backlash, detrimental impact on company’s reputation in the EU, potential complaints (before national DPA) or litigation (before the EU Member State’s national courts), or even collective redress litigation.

- Understand these risks, then get ready to **address them within your company**: compliance with the new rules, adequate communication strategy, EU-specific incident response strategy in place.
F) OUR ESSENTIAL TAKE AWAYS

3.

✓ If your company comes within the scope of application of the Data Protection Regulation, it may become necessary to think of hiring – internally or externally – a Data Protection Officer.
4. Assess *how tough is the DPA in its enforcement actions* in the EU country where your company’s subsidiary is based or doing business (e.g., does it frequently raid or audit companies for data protection violations?; how heavy is its sanctioning power?).
F) OUR ESSENTIAL TAKE AWAYS

5.

✔ Understand what is still uncertain about the upcoming data protection regime, and what is most likely to become mandatory; what will be enforceable right away, and what will not.

➔ Through a gap analysis, address which data security and data breach notification management measures are left for your company to implement.
Cédric Laurant

• Owner, Cedric Laurant Law Firm (http://cedriclaurant.com)

• Attorney-at-Law, Cabinet ULYS (Brussels) (http://www.ulys.net)

• Editor, Blog “Information Security Breaches & The Law” - http://security-breaches.com

• Twitter: @cedric_laurant & @security_breach

• E-mail: cedric.laurant [at] ulys [dot] net & [c [at] cedriclaurant [dot] com.
THANK YOU FOR YOUR ATTENTION!

ULYS, a Modern and Human Law Firm, Dedicated to Innovation!

AREAS OF EXPERTISE
- New Technologies, Privacy & ICT
- Intellectual Property
- Cinema, Media & Entertainment
- E-Payment, E-Finance & Internet Banking
- Sport & Gaming
- Commercial Law

ULYS BELGIUM
224 avenue de la Couronne
1050 Bruxelles
Tel : +32 (0)2 340 88 10
Fax : +32 (0)2 345 35 80

ULYS FRANCE
33 rue Galilée
75116 Paris
Tel : +33 (0)1 40 70 90 11
Fax : +33 (0)1 40 70 01 38

ULYS ISRAEL
Vered Tower, Derech Hashalom, 53
Givatayim
Tel : +972 (0)3 770 70 20
Fax : +972 (0)3 770 70 19

Cédric Laurant
Attorney-at-Law, Cabinet Ulys (Brussels)
(Member of the Brussels and District of Columbia Bars)
[cedric.laurant [at] ulys [dot] net]

www.ULYS.net - www.droit-technologie.org
Presentation (pdf) available at:

http://cedriclaurant.com
&
http://www.ulys.net

On-demand version of the web conference is available at:
https://attendee.gotowebinar.com/recording/6643082475935128320
Open Discussion

Cédric Laurant, Esq.
Attorney
Cédric Laurant Law Firm & Ulys (Brussels)

David Matthews
Director of Incident Response
Expedia, Inc.

James Colby
Vice President
Radware
Closing Remarks

Dr. Bryan Cline
CISO HITRUST Alliance on Incident Response
Thank you, Radware, for making today’s program possible!

Join us again January 31st, 2013

*Budgeting for Governance, Risk, and Compliance*

Visit SecureWorldPost.com for the latest security news and blogs from industry leaders.

Thank you for joining today’s web conference.