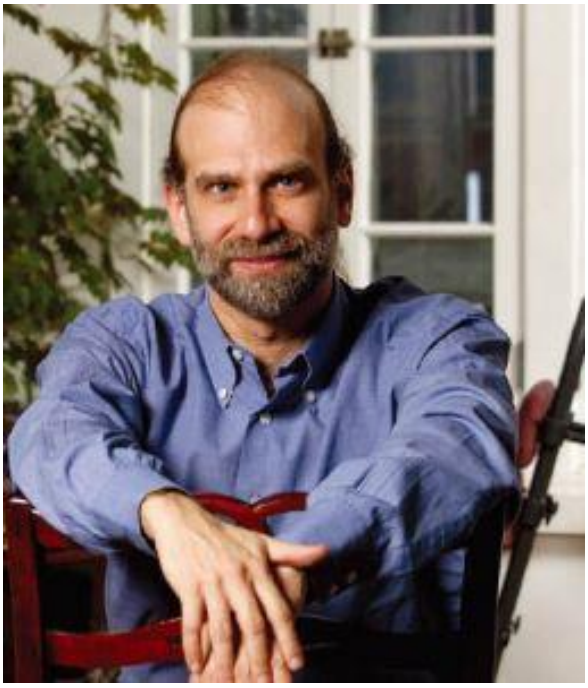
ANTIY 安天技术文献译丛



信息安全事件响应领域的发展现状

Bruce Schneier

摘要

本文主要讲解了信息安全事件响应领域的 3 个网络安全趋势、5 个科学议题以及信息安全事件响应的当前情况，并将它们与美国空军所提出的系统化理论结合了起来。

非官方中文译本 • 安天实验室 译注

信息安全事件响应领域的发展现状

非官方中文译本 • 安天实验室 译注

文档信息			
原文名称	The State of Incident Response		
原文作者	Bruce Schneier	原文发布日期	2014-8-8
作者简介	Bruce Schneier（布鲁斯•施奈尔）生于1963年1月15日，是一位美国密码学家，计算机安全专家以及作家。他撰写了数本信息安全与密码学相关的书籍，并且创办了BT公司并担任其首席技术官。 http://en.wikipedia.org/wiki/Bruce_Schneier		
原文发布单位	2014 黑帽大会		
原文出处	https://www.youtube.com/watch?v=u54Radu2bF0		
译者	安天技术公益翻译组	校对者	@Phreaker（新浪微博）
鸣谢及免责声明	英文版本内容是基于 Bruce Schneier 在 Blackhat 大会上同名演讲报告的网络视频整理而成，安天技术公益翻译组以此为基础翻译了基础中文版。我们的工作获得了新浪微博网友@Phreaker 的全力支持，他发现了相关报告的价值，促成了我们的听记和翻译，并予以了大量校对改译，在此我们表示特别感谢。 特此声明：本文并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。		

信息安全事件响应领域的发展现状

Bruce Schneier

1 引言

今天，我将谈一谈信息安全事件响应，我将谈到 3 个网络安全趋势、5 个科学议题（包括 4 个经济学原理以及 1 个心理学理论）以及信息安全事件响应的当前情况，并将它们与美国空军所提出的系统化理论结合起来。这就是接下来的一小时的安排。【顺便说下，正在进来的朋友，会堂里实际上有很多空座，基本每一排都有。所以，您可以在过道上左右看看，找个座位坐下。防火条例规定大家可以在任何空座位就坐，而不是坐别人的大腿，除非你真

的很喜欢他们。】

1.1 第一个趋势：失控

现在，我们先讲一下网络安全趋势。 第一个趋势是：我们正在失去对我们的 IT 基础设施的控制权。我认为这是非常有趣的现象，因为这是当前新技术运行模式所带来的功能性变化。首先是云计算的兴起，意味着我们对数据的控制能力大大减少，这些数据包括电子邮件、照片、日历、地址簿、信息、文档等。它们都被存储在谷歌、苹果、微软、Facebook 和其他公司的服务器上。可能在这个会场里，仍然将自己数据存储在本地电脑上的人所占的比例是最高的（译者注：Blackhat 会议的参加者大多是信息安全从业人员，比较注重个人数据的保护）。然而，走出这个会场离开 Blackhat 大会，大多数的人都不介意将数据存储在别人的云里面。这就是现在这个世界的运行方式，对个人来说是这样，而且对企业来说也将变成这样。许多公司正将通信服务、CRM 系统、应用系统、计算机桌面外包到云计算环境中。是的，几乎整个 IT 基础设施都被外包到云里面了。当我们这样做时，我们对这些东西的技术细节就失去了控制。是的，我们将无法对这些系统的安全性做出影响。我们采用了虚拟化技术，但对于核心安全性，我们别无选择而不得不对其加以信任，因为虚拟化技术底层的安全性对我们是不透明的。我无法告诉你 Facebook 使用什么样的操作系统。“我不知道，我也不关心”，是不是很多人都是这样的心态？同时，我们也越来越多地我们更加失去控制的设备来来访问这些数据。我们正在使用这些东西【挥舞手中的 iPhone 手机】，iPhone、iPad、Android 手机、Chromebooks...但是与我们的计算机相比，我们对这些设备配置的具体控制能力较低。我如果不破解这些设备，我就不能在机器上运行任意的软件，而大部分人都不会这么做。再看一下操作系统，你审视一下 Windows 8 操作系统，再审视一下 Apple 的 Mountain Lion 和现在的 Yosemite 操作系统，会发现它们都在朝着同样的方向发展，向着厂商控制更多而用户控制更少的方向发展。而且和云计算类似，不仅个人在用这些设备，企业也在用这些设备，仅为大家都觉得需要这些设备，大家都喜欢这些设备。就这样，再一次，导致我们对 IT 基础设施的控制更少了。现在，各公司仅仅处于财务考虑而采取这些措施。从财务角度来看，将所有这些外包出去是很有道理的。这样做费用更低、效果更好，也更可靠...由于这些原因，我们会选择外包的做法。总体来看，在社会上大家都在将基础设施外包出去，而 IT 只不过是在赶上这个潮流。但对于信息安全专业人员来看，这意味着我们对基础设施的控制大大减少。这是我今天要讲的第一个趋势。

1.2 第二个趋势：攻击复杂化

第二个趋势是：信息安全攻击正变得越来越复杂。现在有很多糟糕的新闻，就像大家所知道的，被报道信息更多是新闻编辑们认为有趣的而不是真实的，但我们确实看到了攻击复杂性的提升。现在有各种各样的黑客，比如国家力量、非国家力量、兴趣爱好者、职业罪犯等。而且我们也观察到信息安全攻击在各个层面都变得越来越复杂。我曾经就网络战争提出过争议，而现在人们在谈论其中的一些重大的信息安全攻击攻击事件时，都认为它们是网络战的例子。我认为这是无稽之谈。我认为目前正在发生而且真正重要的趋势是：越来越多战争中的战术行为被应用于更广泛的网络空间环境中。这一点非常重要。通过技术可以实现能力的传播，特别是计算机技术可以使攻击行为和攻击能力变得自动化。曾经的情况是，我们可以通过武器辨别出攻击者。如果你走在大街上，看见了坦克，你会知道，这涉及了美国军队，因为只有军队能负担得了坦克。因此武器能够告诉你攻击者是谁。但是这种辨别攻击者

的捷径在信息安全攻击领域就不存在了，每个人都使用相同的战术行为，每个人都使用相同的攻击技术。这些信息安全攻击覆盖整个威胁谱系。 其中很多攻击属于ＡＰＴ（高级持续威胁）。这是一个我一开始很讨厌但现在开始喜欢的热门术语。我认为这个术语描述一些对ＩＴ安全非常重要但是被业界在很大程度上忽视了的东西。

我们可以通过两个不同的维度来分析攻击者：技能水平和专注度。因此，低技能低专注的攻击者属于“脚本小子”，他们不是机会主义者，他们攻击一切可攻击的目标，就像是为是互联网背景辐射。高技能低专注的攻击行为，包括身份窃取、0day 漏洞利用等这一类常见的攻击行为。低技能高专注的是典型的定向攻击。高技能高专注的则是 APT，即高级持续性威胁攻击。

	低专注度	高专注度
低水平	“脚本小子”	定向攻击
高水平	身份窃取/0day 利用攻击	ＡＰＴ

因为从防御角度来看，我们需要对将这些攻击行为分门别类，不同攻击所需要的防御能力具有差异。在常见的网络犯罪攻击中，决定因素是相对安全性。比周围的人具有更高的安全性，那么你就是安全的。典型网络犯罪的目标只是窃取数据库、信用卡号码，罪犯并不关心从哪里窃取，可以是你也可以是其他人。因此，如果你安全措施比别人好，你就是安全的。

但是对于 APT 来说，出于某种原因，攻击者就是要攻击你，不管你的安全措施比邻居好多少，这时决定因素是你的技术要比攻击者好。我们都知道，那些有动机、有技能和有资金支持的攻击者，最终他们一定能够成功攻击进来。我们都知道有些人以渗透测试为生，也知道他们总能够成功攻击进来。现在的问题是我们要如何处理这些ＡＰＴ攻击。我觉得这些算是有政治动机的攻击，在这里我采用了广义的“政治”概念来定义攻击动机，包括出于民族主义、宗教或道德原因而针对机构和政府的攻击动机。所以，我们看一下那些政治相关行业的公司，比如石油公司、烟草公司、大型制药厂；我们考虑下之前喜欢但是现在讨厌的公司，曾经是微软现在是谷歌。这些都是出于政治动机的攻击者的目标。经济动机的黑客攻击也变得更加复杂，规模更大，具备更充足的资金、而且更加国际化。我认为，真正的情况是：网络犯罪已经最终成熟为一个产业。现在网络犯罪形成了一个完整的供应链：盗贼、销赃、骡子（译者注：专业负责洗钱的罪犯）等等。网络犯罪所需要的一切都可以获得，如果有些东西你无法做到，你就可以将其外包。你可以将这些都串到一起，而从攻击到获利的整个过程已经变得非常迅速和高效。这就是趋势二。

1.3 第三个趋势：政府参与

第三个趋势是政府越来越多地参与参与到网络空间里。政府不了解互联网并任其发展的岁月已经一去不复返了。监管环境越来越复杂。国内和国际上都出现了更多的法律法规，特别是在涉及个人数据的领域，尤其是在美国以外的其它国家与地区。在进攻方面，有很多国家力量支持的间谍攻击。我们知道，几个月前，一些来自中国的攻击者对美国企业发动了攻击。我们也见识过美国和其它国家发动的攻击。在很多时候，各企业的损失仅仅是这类攻击的附带损害，这些企业只是不幸地出现在了攻击者的面前。我们应好好讨论一下关键基础设施，它们可能更多地由政府负责防御。随着各国认识到其电网及交通基础设施都依赖于互联

网，他们会开始说：“我们需要负责其防御”。这样的情况出现得越来越多，另外我们也正在进行网络军备竞赛。现在大约有 27 个国家具备网络战争司令部，他们都在开发网络武器、都在囤积安全漏洞、并都用怀疑的眼光互相审视。然后，他们加倍努力，以确保他们比以前更强大。我觉得，这会导致越来越不稳定。

2 IT 经济学

上述是 3 个发展趋势。现在我想讲一些与信息安全相关的 IT 经济学原理。有 4 个不仅与 IT 也与信息安全相关的经济学原理。我认为，我们对这些经济学原理理解得越多，我们就会越了解发生在我们行业的奇怪的事情。

2.1 第一个经济学原理：网络效应

第一个经济学原理是网络效应。大家都听说过摩尔定律（Moore's Law）。还有一个鲜为人知的定律称为梅特卡夫定律（Metcalfe's law），该定律认为：网络的价值等于用户数量的平方。基本上，网络的价值等于节点之间的两两连接数量。对于真实网络、电话、电子邮件、S&S、Skype 和 Facebook 用户来说，情况确实是这样，而且其原理也非常简单。一台传真机是没用的，仅有两台也没啥用处，但是如果有一百万台传真机，我们就拥有了一个网络。对于电子邮件以及其它的一切，道理也是同样的。越多的人使用系统，则系统就会越有价值。使用 Instagram 的人越多，你就越想使用 Instagram。 这道理对虚拟网络也是成立的，比如 Windows 或 Mac 操作系统用户形成的用户网络，又比如 iOS 或 Android 用户形成的用户网络。虚拟网络中的用户越多，应用程序就会越多；用户越多，机会也就会越多。那么，这说明了什么呢？这种现象意味着：在市场上倾向于出现单一的主导者。这是因为大厂商总会变得更大，而规模大对吸引新用户来说是有意义的。我们考虑几个例子，如 Facebook、Skype、Windows 操作系统。大多数人使用 Windows 是因为他们认识的大多数人在使用 Windows 操作系统。人们使用 Mac 操作系统也是因为他们认识的人在使用 Mac。

2.2 第二个经济学原理：固定成本 vs 边际成本

第二个相关的经济学原理是：固定成本与边际成本。所以，当你看到任何产品时，都存在这两类成本：开发产品的开发成本，以及制造每一件产品的成本。而在 IT 领域，大部分成本都在开发上。以我这顶可爱的帽子为例，它具有设计成本和制造一顶帽子所需要的成本。但是对于我手边的这张 DVD 来说，第一张 DVD 的成本可能是数百万美元，而第二张就是几乎免费或仅仅 10 美分。所以，这是一种奇怪的经济学现象，所有的成本集中于前期的开发过程中，而窃取开发成果是一种非常强大以及有利可图的攻击方式。在这方面，我想到了电影、音乐、制药等行业。等别人付出庞大的成本做出第一个，然后通过窃取其成果来大量制造，这能带来非常高的价值。这就是为什么很多安全措施被投入这个领域，旨在防止这种情况发生。从根本上，我们知道这样的窃取开发成果行为会破坏市场机制，所以我们要人为地采取措施，使其更难成功大规模制造获利，从而使第一个投入开发产品的人能够拿回其开发成本。 在另一些情况下，高昂的固定成本会成为竞争壁垒。以谷歌地图为例，或者说谷

歌街景是一个更好的例子。当有人驾驶着汽车在整个地球上的各个地点行驶并拍照，竞争对手很难做到同样的事情。因此，我们能观察到厂商会大大削减成本并以赶走竞争对手。如果你是这个产品的制造者，当你发现市场中出现了竞争者，你就可以将成本降低至接近为零，而竞争者则难以跟进并抗衡，因为他还没有收回开发第一个产品的固定成本。

2.3 第三个经济学原理：转换成本

第三个 IT 经济学概念与转换成本有关。因此，转换成本是指消费者从一个产品或服务的提供者转向另一个提供者时所产生的一次性成本。在某些情况下，转换成本非常低。你今天喝了可口可乐，但你不喜欢它，那么你明天可以喝百事可乐，转换成本是零。这意味着可口可乐必须具有好的味道，否则你就会喝别的。但有时候，转换成本是很高的。AT&T 今天让我很懊恼，但明天我可能会继续用他们，因为转换到不同的电话运营商代价很高，不仅耗时而且烦人。因为在 IT 领域，从一个产品转换到另一个产品非常麻烦，包括重新培训员工、重新编写应用程序、转换数据等。与我们相关的是：转换成本越高，则转换之前的提供商可能让你越恼火。在转换成本高的行业，通常客户服务就会很糟糕。因此存在所谓的客户锁定概念，客户被锁定着而无法离开。而这就是为什么各行业的公司尽一切所能提高转换成本，常见手段包括使用专有的文件格式、制定外设配件兼容规格，以及在你离开时不让你带走数据。例如，Apple 让你在不使用 iTunes 后很难将你的音乐带走。所有的游戏公司都尽量确保在其他公司的游戏机上不可能玩他们的游戏。15 年前，手机公司努力阻止携号转网，因为重印名片、告诉别人新电话号码的整体开销使得转换成本变得很高。

以上 3 个经济学概念往往会导致一家独大的市场格局。大公司保持其主导局势，或者变得更大。虽然我们不能一概而论，但事实上趋势正是往这个方向发展。

2.4 第四个经济学原理：次品市场

第四个 IT 经济学原理与信息安全尤其相关，这就是所谓的柠檬市场现象，也被成为次品市场。次品市场是由一位名为乔治 阿克洛夫的经济学家提出的，他因此获得了诺贝尔奖。他的研究是市场中的买方和卖方之间的信息不对称情况，特别是，市场中的卖方对产品拥有比买方更多的信息。他采用的具体的例子是二手车市场。他的分析如下：假设市场中有 100 辆二手车，其中 50 辆的价值为 2,000 美元，另外 50 辆是次品价值为 1,000 美元。在这个市场中，汽车的平均价格为 1,500 美元。所有的次品与其它好车一样被卖出去。而他认为，如果市场上的买方并不能区分好车和次品，次品能将好车赶出二手车市场。如果买方不能分辨好产品和一个次货产品，则次品往往会取胜。自从他提出以后，该理论已经被实验和观察方法所验证。这是真实的，而是事实就是这个情况，这就是次品市场。我觉得这解释了 IT 安全行业的很多问题，例如上世纪 80 年代的反病毒厂商、90 年代的防火墙市场、21 世纪初期的ＩＤＳ入侵检测系统市场，赢得竞争的公司都拍胸脯说自己是最好的产品，因为买方无法分辨到底有啥区别。当你审视两个加密产品，它们使用了相同的算法和相同的密码协议，而且它们申明能够提供同样的安全保障，但一个是好的产品，而另一个则是次品。由于你无法分它们的区别，你会买哪一个产品呢？你可能会买便宜的那个产品。

真正的问题是：信息安全的需求并不是功能性的。我们很容易判断文字处理器是否能够处理斜体。我们可以点击斜体按钮，看看会发生什么。这种功能性要求是很容易测试的。而测试加密产品是否安全则非常困难。因此，如果涉及安全性、可用性、可靠性等被我成为称为“Y 需求”（译者注：因为 Security、Availability 和 Reliability 等词汇都是以字母 Y 结尾）

的需求，买方通常难以区分产品的差异。这就是为什么很多卖方在经济学家所说的信号方面投入努力。信号是指卖方告诉买方，他们的产品并非次品的方式。在二手车市场，信号往往是保证书，买方在把汽车开回家后，在一个月内发现并不喜欢这辆二手车，就可以把它退回来并取得退款。在 IT 领域，信号往往是认证、奖项和参考案例。我们的老板们在决策购买 IT 产品的时候，并不太清楚产品到底在做什么，而在寻找他们可以可以依赖的厂商。我记得在 20 世纪 60 年代时有一个说法："没有人因为购买 IBM 产品而被解雇"。就是这个意思：我不知道该买什么，但他们都买 IBM，那我必须买 IBM。现在大家说的最佳实践也是这样：我不知道该怎么做，但大家都说这样做，那我就会这样做。这就是个次品市场。

3 心理学理论

以上是关于经济学的，现在我来谈一下心理学。我会采用一个心理学理论来阐释信息安全，这个理论就是前景理论（译者注：Prospect Theory，前景理论是一种研究人们在不确定的条件下如何做 出决策的理论,主要针对解释的是传统理论中的 理性选择和现实情况相背离的现象），也被称为预期理论。这些也常被称为损失厌恶（译者注：Loss Aversion，损失厌恶是指人们面对同样数量的收益和损失时，认为损失更加令他们难以忍受。同量的损失带来的负效用为同量收益的正效用的 2.5 倍）和框架效应（译者注：Framing Effect，框架效应是指行为者在不同情境下的行为往往遵循不同的行为模式，尤其是以肯定或否定的方式 做出一种选择对后来的选择具有戏剧性的影响）。基本上，这是人类看待风险的一种方式。前景理论中典型的实验是找一屋子的实验对象，一开始时通常是大学本科生，因为这是最容易找的实验对象。然后，将屋子里的实验对象分为两批，让其中一半做出选择：立即得到 1000 美元现金，或者扔硬币决定是否能赢到 2000 美元。这个试验场景很适合拉斯维加斯。如果你调查一下，你会发现，大约四分之三的人会选择确定的事情，即 1000 美元的现金。更多的人宁愿要 1000 美元现金，而不愿为 2000 美元冒险。

实验的第二部分是针对屋子里的另一半试验对象。他们面临一个非常类似的、但有非常不同的选择：马上失去 1000 美元，或者丢硬币决定是失去 2000 美元还是什么都不失去。而事实证明，大约四分之三的人会选择为 2000 美元冒险。这实际上是非常有趣的。提出这个理论的人因此获得了诺贝尔经济学奖，即使他们原本是心理学家。这也吓坏了所有人，因为经济学家说这是不可能的，但是却被一次又一次地验证了。不管是任何时代、任何文化、钱多钱少，都是同样的结果。这些专家已经做了很多验证工作。但基本上，作为一个物种，当涉及收益时，我们都厌恶风险；当涉及损失时，我们都倾向于接受风险。不只是我们人类如此，有人想出了对其他灵长类动物做这个实验，实验结果也基本一致。

关于这一点，有各种解释。我认为最好的一个来自进化心理学。基本上就是这样，如果将自己想象为位于生存边缘的个体，即使很小的收获也意味着你能够活下去。所以，对屋子的第一部分实验对象来说，如果选择不确定的 2000 美元，则一半的人什么也得不到并死去。但是如果选择确定地获得 1000 美元，他们就能够活下去。但是，对另一部分的实验对象来说，确定的失去 1000 美元意味着你会死掉；但是如果选择不确定的 2000 美元，则意味着一半的人什么也不会失去，但是一半的人能够活下去。所以，我们的大脑具备这种偏见。而这个实验的真正有趣的部分是，你实际上会做出完全相同的选择。将其置于收益语境或损失语境之中，仍然可以看到这样的结果。只是一个语义的差异就会造成变化。

所以，这是什么意思呢？这意味着信息安全是很难销售的，因为信息安全永远是这样的选择：购买我的产品因而承担较小损失（译者注：指购买安全产品的投资），或者承担风险而面对更大的损失，即不购买产品防护不足而发生安全事件可能带来的损失。大家可能已经

遇到过这种情况。当你对老板说：“我们需要购买这个安全产品，因为我们面临着很大的风险”。老板看着你，说：“上个月我们也没有使用这个产品，但是什么事也没发生。也许我们应该碰下运气”。是这样吧？我们倾向于将筹码压在损失不会发生上。

3.1 人员、过程与技术

这个心理学理论如何影响信息安全事件响应呢？

我们都知道，安全是预防、检测和响应等三个步骤的组合。我们需要响应是因为预防不可能完美。如今我们越来越多的需要加强响应，这是因为：

第一，我们已经失去了对计算环境的控制，有很多防护机制我们无法实施；

第二，攻击正在变得越来越复杂，我们需要更多的响应措施；

第三，我们越来越多地被卷入其他人的战斗中；

第四，在我们生活的现实世界里，企业对信息安全防护和检测措施的投资往往不足。

虽然在 20 世纪 90 年代，我常说信息安全是一个过程而不是一个产品，这是非常战略层面的，我的意思是：你不可能购买一堆产品，然后就认为万事大吉了。你必须不断地评估你的安全，并不断重新评估、重新调整你的立场。但从战术层面上看，信息安全成为了一种产品和过程，它实际上涉及人、过程和技术，就像我在 21 世纪初常提到的。真正变化的是过程与产品的比例。IT 安全领域的传统观念是：人员一般不会带来帮助。人员成为了一种负担，人员需要被从系统中挪开。我引用 Lorrie Faith Cranor 的话：只要有可能，信息安全系统的设计师应该将人员排除在循环之外。我们都了解这一点，人员是一个问题，是最大的信息安全问题。而且，我们在这方面已经做得很不错了：完全自动化的防御系统、反病毒与补丁升级、大量的自动化和半自动化检测系统。我们把人员拽出了循环，而且做得相当不错。

但是信息安全响应面对的问题是：我们无法实现完全自动化。我们不能将人员从循环中移除掉。通过仔细考虑可以发现，从防护与检测转向响应，人员所占得比例与技术相比会有所上升。由于各种原因，我们不得不需要更多的人员和相对更少的技术。所有的攻击都是不同的，所有网络是不同的，所有的安全环境是不同的，而且所有的组织也是不同的。组织所处的监管环境是不同的，各个国家的政治经济因素是不同的。这些差异往往比技术因素更重要，这会在经济学角度影响 IT 安全。

信息安全响应所对应的产品和服务是不相同的。响应对网络的影响比较小，有则更高的边际成本，但是转换成本较低，而且在次品市场上出现的较少。这将是很有趣的，因为这意味着，与 IT 安全的其他很多领域不同，更好的产品、更好的服务、更好的厂商会做的更好。这样就减少了先发优势，自然垄断也少得多了。这在我们行业中是新鲜的，这可能是一个惊喜，我认为这是一件好事。我觉得我们都会从中受益。所以，对于人员、过程和技术的三方面，关键问题要使其能够实现规模化。所以，我再次引用 Lorrie Cranor 的话：然而，对于一些任务，依靠人员提供可行或具备成本效益的替代方法是不现实的。她表示，我们将会有一个预算限制。在这样的情况下，系统设计师应当采取工程化手段使这些系统能够支持在响应循环中的人员，并将这些人员成功执行关键安全功能的能力最大化。因此，在不能从循环中移除人员的情况下，你必须开发技术以支持人员执行关键任务。我们可以参考一下应急响应系统、警察、消防、医疗、军事等，这些都是技术在发挥作用的领域。在响应系统中，技术支持承担关键任务的人员；在 IT 安全响应中，我们需要使用技术来辅助人员，而不是反过来。

3.2 应变恢复能力

在这里，我们的目标是提升应变恢复能力，而且值得强调的是我们要建设具备应变恢复能力的系统。我们不会去尝试建设坚不可摧的系统，当然也不应该建设脆弱的系统。很多信息安全响应的策略也与应变恢复能力相呼应，例如缓解策略、生存性策略、可恢复性策略、适应性策略等。这些都是实现应变恢复能力的方法。

3.3 OODAL 反馈循环

在 IT 领域中，信息安全响应与空战最为相似。他们都与反馈循环有关。美国空军有一套非常好的系统理论来论述这一点，这实际上来自空战领域，即 OODAL 循环。我们将在 IT 领域讨论 OODAL。虽然过度使用这个军事概念是危险的，但我认为这个概念具有非非比寻常的价值，所以值得我们深入思考一下。

OODAL 代表观察（Observe）、调整（Orient）、决策（Decision）、行动（Action），而且是一个循环。这套系统理论是由空军军事战略家约翰·博伊德开发的，他为空战开发了这一理论。空战中的飞行员在脑海中不断地经历 OODA 循环：观察、调整、决策和行动。这是一个收集信息、评估决策和采取行动的过程。这种类型的过程已经被广泛应用在各种实时对抗的场景中。有些文章不仅探讨飞机空战，还谈论了军事战略规划、企业竞争等各个领域的应用。

根据定义，这是一个重复迭代的过程。处于这种场景的人在脑海中不断重复这一循环。博伊德发现速度是至关重要的，如果你的 OODA 循环比对手更快，如果你能“进入”对手的 OODA 循环，那么你将会获得巨大的优势，你可以在对方做出反应前更快更有效地进行响应。有些不错的文章介绍了将 OODA 循环应用于网络安全和响应。我推荐大家查阅一些相关论文，可以谷歌一下这个术语并了解一些相关内容。

我喜欢这个框架的原因是，它为我们提供了讨论信息安全事件响应所需要的有效工具的一种方法。事实上，我们现在急需有效的工具。我们需要优秀的信息安全事件响应工具，以便于执行所有的步骤。将这些步骤分解来看：第一步是观察，实时了解我们网络中所发生的事情。所以，这包括实时检测威胁的 IDS、日志监控与分析工具、网络性能分析工具、网络管理工具、物理安全信息监控等，几乎包括所有的一切。无论是攻击之前还是攻击过程中，我们或许都需要把所有的数据集中到一起并进行实时监控。

第二步是调整，需要了解信息在上下文环境中的意思，这对于响应来说是至关重要的。企业等组织中的上下文环境信息包括：当时公司正在发生什么事情？更大互联网社区的上下文环境如何？有什么样的恶意软件正在传播？观测到了哪些 0 Day 漏洞？处于什么样的地缘政治局势中？是否有一些刚刚发现并被公布的新漏洞？企业是否正在推出新的软件产品？公司正在计划裁员？有没有发生并购？之前有没有出现来自该 IP 地址的攻击？网络是否曾经向合作伙伴开放过？这几乎包括了所有的信息，包括来自于新闻、情报订阅以及组织内部各个方面的信息。简而言之，就是在上下文环境中找出到底在发生着什么事情。

第三步是决策，即确定应该做什么。这实际上是很困难的。谁有权做出决策？他们如何做出决策？需要管理层输入什么样的信息？是他们的营销数据？是他们的公关数据？是他们的法律数据？你怎么证明决策是合理的？因为事后，可能需要在一些调查机构（无论是公司内部还是在法律诉讼中）证明你为什么这样做。这是决策过程。

第四步是行动，即能够在网络上迅速做出应变。有不少公司在这方面失败了，因为他们的信息安全事件响应团队的人员无法得到作出应变修改的授权，他们可能没有足够的权限。

在需要进行修改之前，我们不知道他们需要什么权限。响应团队需要能够接触各种 IT 产品并接受持续培训。我们需要为这些工作配备工具，我们需要强大、灵活、直观、能够帮助我们完成任务的工具。这不仅仅关系发到个别的领域，这保护是信息安全事件响应产品和服务的一套完整生态系统。信息安全事件响应变得日趋重要，其原因包括很多方面：攻击更加复杂、监管环境正变得越来越复杂、缓解手段使用的越来越多、地缘政治因素重要程度提高，以及企业对信息安全防护了解得越来越深。

我对未来几年的发展会比较乐观。原因是信息安全事件响应软件不会其它信息安全解决方案一样沦为“Y 需求”。我刚刚提到的那些方面，它们都不仅仅是非功能性要求，它们都是产品和服务必须做到的。这意味着好产品将会击败平庸的产品。而我们作为工程师需要开始开发好产品，因为这是非常重要的。我已经开始在一家名为 Co3 Systems 的公司着手开发产品了。我试图建立一个管理平台来协调信息安全事件响应，这只是一部分。重要的是核心部分，但需要添加很多内容。它必须能够融入很多东西，能够相互合作。我们的目标是以一种前所未有的方式把人员、过程和技术结合起来。我们将更多借鉴通常的危机管理方法。我们可以从很多传统领域中借鉴到有意义的经验，这些领域在几十年来一直在做着类似的事件响应工作。这就是我们将要对抗信息安全威胁的方法。

4 问答环节

下面，大家可以提问了。一般的情况是，只要有一个人举手，其他人就会跟着举手。因此，需要有人做第一个吃螃蟹的人。

4.1 【问题：关于事前防护】

我不知道。我的意思是，很长时间以来人们面临投资不足的情况，而且形成了很多框架。我不知道会不会出现好转，但我认为，从根本上来说，我们将始终面临投资不足的问题。对攻击进行响应，比在攻击前投资防护措施来得更加有效。当你取得了成效，目标被聚焦了，管理层等人群才会被效果所触动。但是我们将始终处于投资不足的情况，并只能在事后尝试解决问题。一个很基本的问题是，我们都是人（译者注：指人类对风险的理解特点），我们该怎么办呢？所以，对于这一点我并不抱很大希望。

4.2 【问题：关于自动化响应】

我不认为可以实现自动响应。响应太过战略性了，它不像补丁，我们只需要安装补丁就行了。响应很大程度上依赖于人员，包括防御和合作。您可以将其他事情实现自动化，例如获得数据和输出数据。当你弄清楚该怎么做时，你就可以将其自动化，但是仍然需要进行分析和确定，这就需要人脑了。因此，单个部分可实现自动化，这是有意义的。但是，事件响应的实际过程将总是需要人员团队。现在，公司可以外包这一团队。有很多公司可以帮你处理 IT 基础设施，包括事件响应。但是他们需要跟你沟通，因为这是你的业务。所以，不，我认为我们无法将人从循环中移除。当我们创造出人工智能时，也许可以。但在此之前，是不可能的。

4.3 【问题：关于反击】

关于反击的问题，我真的不赞同反击。我的意思是私自执法在我们的社会中并不能带来良好的效果。我认为我们将会看到很多企业越来越希望进行反击，因为他们受够了遭受攻击的被动情况。但时如果要进行反击，你必须定位攻击的来源，并对他们的网络进行攻击。但事实上在反击方面，我们有很多的麻烦。有时候，我们可以找出攻击源，但需要数周或数月。著名的安全研究公司 Mandiant 也需要一段时间才能产生报告。但为了反击，你必须在毫秒之内找出谁发起攻击。所以，我认为反击并非是一个好的解决方案，我认为这是一种危险的趋势。我真的不看好它，因为这样太容易出错，很容易反击到无辜者。

4.4 【问题：关于政府参与】

关于政府对安全的合规要求，有很多问题。我认为这正在发生，尤其是在相关行业中。就像政府对食品安全的合规要求一样，我们将会看到政府对数据安全提出要求。这将取决于，例如美国、欧洲等政治因素。但是，在其它领域，诸如此类的安全要求，特别是对安全的底线要求是很常见的，它们最终也会进入 IT 领域。我不确定这是不是一件好事，我认为这种情况就要发生了，我认为政府说：“让业界自行处理”的时代即将结束，以后将会有更多的政府干预，将会有各种水平的政府接管或安全、税收优惠、FDA（美国食品药品监督管理局）或 FTC（美国联邦贸易委员会）、处罚和规则依赖于政治。但我认为更多的政府干预就要来了。

4.5 【问题：关于传统领域】

我们看到有些企业的响应做得非常好。它们往往来自于一些传统行业，这些行业远在计算机出现之前就在处理灾难事件。例如石油和天然气行业，公司需要应对飓风。事件发生后，他们擅长召集一个应急团队，并确定该怎么做。对于 IT 领域来说，只是技术在大型体系中的一个应用。所以，IT 领域的人可以从其他领域借鉴经验。再次，我认为这是一个很好的事情，会看到很多的跨界发展。

4.6 【问题：关于云计算安全】

关于云计算公司以及他们如何寻求安全。这是很有趣的，对于大型云计算公司来说，它们的安全模型是“信任我们”。如果想将电子邮件外包给谷歌，你去谷歌，说：“我们需要审核电子邮件系统”，他们会拒绝；如果你说“我们想使用你的服务”，他们才会说 OK。所以，他们的模式是要么接受，要么离开。而且他们规模大，足以做到这一点。不过一些规模较小的云计算服务公司也有愿意接受一定的安全审核。我认为会出现某种瀑布模型。这种成熟的方式是：你将基础设施外包给 Rackspace 公司，Rackspace 公司将会接受并审核。你可以得到一份审核副本并将其添加至你的审核中。然后，你将这一副本提供给使用你基础设施的人，他们也将该副本添加到他们的审核中。我认为，事情将会这样发展，但还需要一段时间才能实现。我认为没有其他的方法。目前还没有任何强制审核要求，也没有公司允许别人审核他们的东西。但是，他们可以给你一份审核报告，说：“我们已经被审核过了，这是结果”。所

以，你可以使用这些数据满足自己的监管机构。我认为这种模型就要到来了。

4.7 【问题：关于事件响应】

关于事件响应的问题。企业怎么能与具备优势资源的攻击者竞争呢？也许不能。攻击者将会进入你的网络。问题是以后发生的事情，而这并不总是钱越多的人能够赢。它与我们的风险厌恶态度有关，与法律环境有关。当出现“我无法与比我更厉害的黑客对抗”时，企业可以选择报警。这是一个方法，企业可以暂时得到更多的资源。所以，在与比我们更熟练、可怕强大的攻击者对抗时，我们有很多教训。我们希望将它们应用于此。在一般情况下，我认为有更多资源的攻击者总会进入。现在的问题是我们如何将他们踢出去、如何恢复安全、如何通过 OODA 循环实现应变回复。这是响应的整个概念。我们正在响应，因为攻击者已经闯入我们的网络、我们不是响应潜在的攻击，而是实际攻击。而且，有很多事情是我们可以做的，而不应该说“他们进来了，所以我们完蛋了”。

4.8 【问题：关于应变恢复能力】

关于应变恢复能力，我是指：我们如何维护、如何缓解威胁、如何减少损失、如何生存下去、如何确保我们不会就此崩溃、如何恢复、如何将攻击者踢出去、如何恢复安全、如何适应、如何不断完善自己使我们的安全性更好，这真得很难。所以，我认为应变恢复能力包含方方面面。另外，这是一个不同的“Y 需求”的重要需求，我们需要确保即使面临攻击者时我们也是安全的。有很多这样的例子，作为一个物种，我们能够从疾病中恢复过来。疾病会杀了一些人，但不会杀死所有人，我们的遗传多样性就是我们抵御疾病的安全机制。这对 IT 来说并不是一个好策略。“百分之十的人会被病毒感染，其余的人将会活下去”，这种方法是很糟糕的。但是，物种就是这样的。所以，我认为一个更广泛的办法是使用一揽子威胁应对手段来构建安全体系。

4.9 【问题：关于赏金计划】

我觉得赏金计划是很有趣和有用的，我并不确定是否有效。不幸的是，目前军用市场和黑市的价格都比漏洞赏金高，这对于人们是很有吸引力的。这种计划有一定的帮助性，现在很多公司都认真地采取这种方法。但是，越来越多的网络武器和武器制造商发现缺陷却不把其上报，因为出售给世界各地的政府可以赚更多的钱。所以，虽然我喜欢这些计划，我认为它们是很好的，只是没有真正抱着希望。这是令人沮丧的。

4.10 【问题：关于前景理论】

关于前景理论的问题。我们如何帮助人们改变思维方式？这是很难的。一般来说，克服心理偏见的方法是了解它们并予以弥补。我们知道，当涉及收益时，我们规避风险；当涉及损失时，我们“勇于”冒险。理论上你可以观察自己的行为并进行弥补，但正如赌场中一直存在的那样，如果你知道这些偏见，你可以走过这些赌桌，看着那些祈祷赢钱的赌徒们说：“这对不懂数学的人在征税呢，继续吧”。因此，我们克服这些困难的办法就是通过了解它们，但这是很难的。我们知道，对恐惧的恐慌会导致大量的心理偏见，甚至一个国家都会完全坠

入其中。我们应该谈论它们，思考它们，并希望能够克服这些偏见，这是可能的。而且这不止是 IT 领域，对吧？人们试图通过恐惧来销售保险和防盗报警设备。是的，通常情况下，购买防盗警报设备的，大多是是遭受了抢劫或邻居被抢劫了的人，他们就是在此时购买防盗警报。

4.11【问题：关于误报】

误报确实破坏了很多系统。在这方面，我们现在做得更好了。检测技术仍然有很大的提升空间。响应措施也可以是你做的其它事情，当谈到响应时，我指的是我们需要能够迅速理清并排除误报的方法。我给出两个例子：一个是机场安全，你走过金属探测器，突然警报响起，这时候检查人员会快速弄清楚发生了什么事情，如果它是一个误报，他们就会很快从中学习到经验。在另一方面，如果国家安全局告诉联邦调查局恐怖袭击情报，比如在 911 后他们发了 10,000 多个文件给联邦调查局，而联邦调查局的人员需要花费几百个人时的工作量来清除每个误报，这样的成本非常高。因此，重点在于需要通过二次测试迅速清除误报。如果你能做到这一点，那么你就可以更快更轻松地进行主要测试。我们基本上就是这样处理医疗测试的。所以，这就是我们所需要的东西。

所以，非常感谢大家参会。我会在这里，我很乐意与大家交流并签名。

附：英文原稿

The State of Incident Response

Bruce Schneider

So, I'm gonna talk about incident response. I'm to talk about the mean of fashion. I'm gonna talk about three trends in cyber security and talk about 5 pieces of science, 4 economics in psychology, talk about the current status response and try to tie this all together with some systems theory from the US Air Force. That's the plan for the next hour. And again, if you are coming in, there are actually lots of seats all around. Probably in every row, there exist one seat. So, if you just come down the aisle and look left or right to find a seat and sit down. And the fire codes say you can sit in any empty seat, and you can't seat on someone else's lap unless you really like them.

Right, so trends first. First, the trend is that we're losing control of our IT infrastructure and i think is really interesting to watch because it's really a function of the way technologies are working right now. The first thing that's happening is the rise of cloud computing, meaning we have a lot less control of our data, right, our email, our photos, calendar, address book, messages, documents. But they're all on servers belonging to Google, Apple, Microsoft, Facebook and other different companies. Now, probably in this room is gonna be the greatest concentration of people who actually still have their stuff on their computers. Go out of this room, out of this conference, everybody else is going to have their data on someone else's cloud. And that's the way the world is working. It's true for individuals. It's also becoming true for organizations. Many organizations are now outsourcing communications, CRM systems, applications, desktops, right, the entire IT infrastructures into the cloud. And as we do that, we lose control over the tech details of those things. Right? We often can't affect the security of those systems. We can bring virtualization, but the core security we simply have to trust, like i don't have visibility in the security. I can't tell you what kind of operating system Facebook uses. I have no idea, and I pretty much don't care. Right? And also we increasingly accessing all this data through devices we have much less control. Right? We're using these things, iPhones, iPad, Android phones, Chromebooks, where we don't have as detailed control of the configuration as we do on our computers. Right? I can not run arbitrary software on this machine unless I break it, which normal people are gonna do. And if you look at the operating systems, you look at Windows 8, you look at apples now apply. Both of those are moving in the same direction. Of more vendor control, less user control. And again, corporations are using these things just as much as individuals are, because people want them, people like them. So, I get so again, less controlled infrastructure.

Now, organizations are doing this for personal financial reasons. Right? It makes a lot of sense to outsource all these. It's cheaper, it's better, and more reliable, all the reasons you do it. And in general, we in society always outsource infrastructure, like IT's we are catching here. But as security people, this means we have much less control. That's the first trend.

Second trend, attacks are getting more sophisticated. Now there's a lot of, seems there are a lot

of lousy news out there. You know, what's reported on seems to be a function of what editors find interesting and less what's real, but we are seeing an increase in attacker sophistication. By this Friday, nation-state, non-nations, hobbyists, criminals, and we are seeing increasing sophistication across all levels. I have debates on cyber war and now people are talking about some of these major attacks as examples of cyberwar. I think that's nonsense. I think that's really going on and the really important trend is that we're increasingly seeing warlike tactics being used in broader cyber context. This is important. Technology spreading capability, especially computing technology, which can automate attacks and capabilities. And it used to be you could tell the attacker from the weaponry. And if you walked outside on the street and you saw tanks, you knew that the US Army was involved because only armies could afford tanks. Right? The weaponry told you who the attacker was. That shortcut doesn't work anymore. Right? Everyone is using the same tactics, everyone is using the same technologies all across the broad spectrum.

So, a lot of this is advanced persistent threats, a buzzle word that I started out hating and have come around to like. I think describing something is really important. About IT security, that is as an industry we've largely messed. See, you could think about attackers along two different axes: skill and focus. So, low skill low focus attacker, that's the script kiddie, that's the opportunist, that's someone that is attacking everything and anything. I want to think it as the background radiation at the Internet. High-skill low focus, think those identity theft attacks, zero-day exploits and the kind of stuff we also see pretty regularly. A lower skill high-focus is the typical targeted attack. High skill high focus, that's APT, that's advanced persistent threats. And the difference, the reason this is an important distinction is that the defensive posture became the defense. The way you look at your defense is different. In a normal criminal attack, what matters is relative security. Have your security better than the people around you, you are safe. The typical criminal once wants a database, a credit card number, doesn't matter where he gets it, it'll be you or somebody else. If you're better, you're fine.

Against an APT, the attacker for some reason wants you, and there doesn't matter how much better you are than your neighbors. What matters is are you better than the attackers. And we all know in this room, that the attackers officially motivated, skilled and funded, they will get you. You all know somebody does pentesting for a living, and you know they never fail not to get it. Right? The question is how we deal with it. I think this is politically motivated attacks and I define politics very broadly here, nationalistic, religious, ethical institutions and governments. So, you think I want to know companies in politically-charged industries, big oil, big tobacco, big pharma. You think of the companies i used to love but now hate, used to be Microsoft now it's Google. These are the targets of politically motivated attackers. Financially motivated hacking is also more sophisticated, made bigger, better funded, more international. I think what's really happening is that cybercrime is finally matured as an industry. Right? There's now an entire supply chain in spades in place for cybercrime, thieves, defenses, mules, all the pieces. There is anything you can't do, you can outsource. You can chain it all together, and the process from the attack to monetization has become very fast very efficient. That's trend 2.

Trend three is the increase of government involvement in cyberspace. Right? Long gone are the days when governments didn't understand the Internet and when they left the internet alone. The regulatory environment is getting much more sophisticated. This is domestically and internationally a lot more rules involving personal data, especially outside the US. On the attack

side, there's a lot of nation-states sponsored espionage attack. You know we're seeing which dates back a few months ago, some attackers from China against US corporate targets. We're seeing nation-state attacks conducted by the US, by other countries. And a lot of time, organizations are really collateral damages, they are sort of in the way more than anything else. There's a lot more to talk about critical infrastructure, which could be more government-run defense. As countries realize that their power grid and their transportation infrastructure are all dependent on the Internet, they are gonna start saying: “hey, we need to be in charge of its defense". The thing is there's more and more. And also, we have a cyber arms race going on. There's like twenty seven countries now with cyber commands. They are all building cyber weapons, they're all stockpiling vulnerabilities, and they're all looking at each other with suspicion. And then, doubling their efforts to make sure they are stronger than before. And I think this is increasingly destabilized.

Those are the trends. Now I want to give you some IT economics that's relevant to security. So, I have 4 pieces of economics that matters for IT, matters for security. I think the more we understand them, the more we understand the weird stuff that happens in our industry. The first one is network effect. Oh, you've all heard of Moore's Law. There's a lesser known law called Metcalfe's law, which says that the value of the network equals the square of the number of users. Basically, the value of the network equals the pairwise connections between the nodes. This is true for real networks, phones, emails, S&S, Skype, Facebook users, and the intuition is pretty simple, right? One fax machine is useless, two are boring, have a million, and suddenly we have a network. Right? It's the same for emails, for everything else. The more people that have the system, the more valuable the system is. The more people on Instagram, the more you want to be on Instagram. This is also true for virtual networks. The network of Windows verses Mac users, IOUs verses Android users. The more people in the virtual network, the more apps, the more you as a group, the more stuff happens. So, what does this means? This phenomenon means you tend to have a single dominant player in the market place because the big get bigger, because being big is valuable to the new users. Let's think about Facebook, thing about Skype, think about Windows. And most people run windows because most people know are Windows. And people are on Mac because people know Mac.

The second economics that is relevant is the notion of fixed costs verses marginal costs. So, when you look at any product, these two types of costs as the development costs to develop the thing and the costs to make each individual think. And in IT, most costs are in development. This wonderful hat of mine has design cost and the cost from making another one. But for this thing, wherever it is around just got here, right? The cost for the first one might be a bunch of million dollars, and the second one is free, 10 cents. It's a DVD. So, this weird economics, and all the costs to the thing is front-loaded in the development, means stealing the result of the development was a very powerful attack. I think of movies, think of music, think of pharmaceuticals. Being able to make a lot of these and have someone else pay to make the first one can be very valuable. And this is why you see a lot of security going into making this not happen. And fundamentally, you know mechanisms that break the market so we have to artificially make it harder to make a lot of these, so whoever made the first can recover its money. In other cases, the high fixed costs could barrier the competition. I think of Google Maps. Thank you, google street views is a better example. Someone drives the car around the entire planet, taking pictures. It's much harder for a competitor do the same thing. And then you have these dynamics. With them, vendors will cut

costs dramatically to drive out competition. Right? So, if the maker of this thing, she's a competitor on the line. They can drop their costs almost to nothing with a competitor who can't compete because he hasn't recovered is fixed costs yet.

The third piece of IT economics matters a lot of the notion of switching costs. So, switching cost is the cost to switch to a competitor's product. In some cases, switching costs are very low. You drank a coke today and you didn't like it. You can drink a pepsi tomorrow. The switching cost is zero. That means the coke has to taste good or you're gonna switch. Sometimes, switching costs are high. Right? AT&T pisses me off today, and i am likely gonna keep them tomorrow, because getting a different phone carrier is expensive, it's time-consuming, it's annoying. Because in IT, switching from one product to another can be a lot of things, retraining staff, re-writing applications, converting data. What's relevant to us is that the higher the switching costs, the more the company can piss you off before you switch. Right? In this resort, our switching costs are high, customer service is lousy. Because you have this what's called locket, by which customers are locked in. And this is why you have in our industry companies doing everything they can to keep switching costs high. Right? That includes proprietary file formats, compatible accessories, not letting you take your data with you when you leave. It's really hard for you to take your music with you when you leave iTunes. All game companies want to be very expensive or impossible for you to run the games on someone else's console. A good decade and a half ago, the cell phone companies fought really bitterly cell phone number portability, because the whole cost of you reprinting your business cards, telling people you new phone number kept the switching costs high.

All these three things tend to lead to a dominant market structure. A big gets bigger and big stays big. It's not guaranteed, but these are trends in that direction.

A fourth piece of IT economics is especially relevant to security. It's an ocean at the lemons market. So this is work by a economist named George Akerlof, and he won a Nobel Prize for this. And what he studied was markets with asymmetric information between the buyer and the seller, specifically, markets where the seller knew a lot more about the product than the buyer. The specific example he used was a used car market. And this is his thought analysis, suppose there is a town with 100 used cars for sale, fifty of them cost two thousand dollars, and fifty of them are lemons that cost one thousand dollars. In that market, the median price for a car is fifteen hundred dollars. In that market, all the lemons sell another good car sell. And what he proposed is that in a market where the buy can't tell if it's been a good car and a lemon. Lemons try as good cars on the market. When the buyer can't tell apart a good product and a mediocre product, the mediocre products win. And since he came up with this theory, it's been verified experimentally, it's been verified observatially. This is true. This is what happens. This is the lemons market. I think this explains quite a lot about IT security. You think about the antivirus companies of the 1980s, the firewall of the nineties, the IDS of the 2000's. The companies that won warrants the best products. Because the buyers couldn't tell the difference, I can hold up to encryption products they use the same algorithm, same protocol where they make the same security claims. One is really good and one is kinda mediocre. You can't tell the difference. What's you gonna buy, you could buy the cheaper one.

The real problem here is that the requirements are non-functional. Right? It’s easy to tell if a

word processor does italics. You had the italics button, and can see what happens. That is a functional requirement easy to test. Whether encryption product is secure is much much harder to test. So, security, availability, reliability, what I think it is the Y requirements, buyers have trouble telling the difference. And this is why you see a lot of efforts going into what economists call signals. Signals are ways sellers say to buys that their products were actually not lemons. The used car market they tend to be warranties. Take the car home, drive for a month till, you don't like it, bring it back and give your money back. In IT, signals tend to be certifications, tend to be awards, references. All the way that our bosses by IT products. Not quite knowing what they're doing but you're finding someone else that they can rely on. I remember in the in the 1960s, no one ever got fired for buying IBM. That's what that meant. I don't know what to buy but they all buy IBM, I must by IBM or today's best practices. I don't know what to do but everyone says do this so I'm gonna do this. And that's a lemons market.

All right, that's the economics. Now my one piece of psychology. I'm gonna try to explain security in terms of one psychological theory, and the theory is prospect theory. And you'll also hear this codes: loss aversion, framing effects. Basically, it is a way that we as humans look at risk. The quintessential experiment in Prospect Theory is to take a room full of subjects, you know, in the beginning it usually college undergrads, because that's what we got. Then, you divide the room in half, and you ask one side of the room to make a choice, and the choice is between a thousand dollars in cash and a flip in two thousand dollars, kind of appropriate experiment for Las Vegas. And if you survey the people, you will find that about three-quarters will take a sure thing. More people would rather have a thousand dollars than a flip chance to two thousand dollars.

Second half of the experiment is for the other half of the rooms. You get a very similar but importantly different choice. I can either take a thousand dollars from you right now by take a bank account or I will let you have a flip chance at me taking two thousand dollars or nothing. And it turns out if you ask a room full of people to make that choice, about three-quarters of them will take the chance. Now this is actually really interesting. Are the people who came up with this theory also won a Nobel Prize in economics even though they were psychologists? Freaking out everybody because economists said this is impossible yet this has been proven again and again. And it's very robust result across ages, across cultures, done with little money, with real money. I mean these experts have been done a lot. But basically, as a species, we are risk-averse when it comes to gains and risk seeking when it comes to losses. That is not just us. Someone figured out how to do this experiment on other primates. And we kind of all are.

There's been a bunch of explanations up this. I think the best one comes from evolutionary psychology. And this is the basic story. If you imagine yourself as an individual living at the edge of survival, even a small win means you live to see tomorrow. So, over this half of the room, if they take flips at two thousand dollars or nothing, half of them will get nothing and die. But if they take a sure thing a thousand dollars, they'll live. But this half if the room also living at the edge of survival, a sure loss of a thousand dollars means you will be dead. But a flip of two thousand dollars means half of you lose nothing, half of you survive. So, our brains are primed to have this bias. And the really interesting part of this experiment is that you actually take the exact same choice. Frame it in the language of gains or the language of losses, and you still see the result. Even just a semantic difference causes the change. So what this means? It means security is hard to sell, because security is always a small loss buying my product versus a risk and a larger loss,

what'll happen if you don't have the product. And you've probably experience this. When you went to your boss and said: “hey, we need to buy this security thing because we're at the risk of this even bigger bad thing”. And your boss looked at you and said: “we didn't have the product last month and we didn't have the bad thing last month. Maybe we should take the chance”. Right? Avoiding losses is how we work.

Okay, so how does this affect incident response?

So, we all know that security is a combination of protection, detection and response, three steps. And we need response because protection isn’t perfect. We need it more and more today especially because: One, we've lost control over computing environment, there’s lot of protection we can’t do. Two, attacks are becoming more sophisticated. We need more response. Three, we increasingly parts of other people's fights. Four, we're living in a world where companies will naturally under-invest in protection and detection. But in the 1990’s, I used to say security is a process not a product. And by that I meant something very strategic. What I meant is that you can't buy a bunch of stuff then be done, you have to continually evaluate your security, and continually reevaluate, repurpose your stance. Tactically, security becomes a product and a process. It’s really people, process and technology. Right? Now something I used to say in the early 2000's. What’s changing are the ratios. The conventional wisdom in IT security is that people don't generally help. Right? People are a liability, people made you remove from the system. I have a quote from Lorrie Faith Cranor. She writes: whenever possible, secure system designers should find ways of keeping humans out of a loop. Great. Okay, keeping humans out of a loop. We all know that. People are a problem. People are the biggest security problem. And, we’ve been doing pretty well at this. The entirely automated prevention systems, anti-virus patching, lots of automated and semi-automated detection systems. Right? We are pulling people out loops, and we are doing it pretty well.

The problem with response is that you cannot fully automated. Right? You can't remove people from the loop. And if you think about it as you move from protection and detection to response, the people to technology ratio goes up. Right? You need more people and less technology for a whole bunch of reasons. Right? All attacks are different, all networks are different, all security environments are different, and all organizations are different. The regulatory environments of organizations are different, the political economic considerations of your nation are different. Those differences are often more important than the technical considerations. This affects the economics about IT security.

Right? The products or services for response are different. There are less network affects, there are much higher marginal costs, there are lower switching costs, and there's less on the lemons market. This will be interesting for us because it means that unlike a lot of other areas in IT security, better products, better services, better companies will do better. This lessens first-mover advantage. There are far fewer natural monopolies, and again, this is a new thing for us in the industry. This can be a surprise and I think it's a good thing. I think it's something we're all gonna benefit from. Right? So, people, process and technology. The key here is making its scale. So, I'm at the following sentence from Lorrie Cranor. She wrote: however, there are some tasks for which feasible or cost-effective alternates from humans are not available. She means we'll have a budget. In these cases, system designers should engineer these systems to support the humans in the loop and maximize their chances for performing this security-critical functions successfully. So in

places where you can't remove humans from a loop, you have to build technology to support humans in their critical tasks. Thinking of any emergency response systems, thinking of police, thinking of fire, thinking of medical, thinking of military. That's what technology does. Technology supports the humans who are critical in their response system. Right? In IT security response, we need technology to aid people and not the other way around.

And the goal here is resilience, and very strongly the goal here is to build the resilience systems. We're not gonna build impenetrable systems, and we shouldn't build fragile systems. And a lot of response strategies echo resilience, right, mitigation, survivability, recoverability, adaptability. These are all ways to achieve resilience. And because responses is the closest thing we have in IT to dogfighting. This is all about feedback loops. And there is a really nice piece of systems theory coming from the US Air Force that talks about this. Actually comes from dogfighting, and notionally OODAL loops, and OODAL loops aside to be talked about IT. It is a danger we're going to overuse this concept but I think it's extraordinarily valuable, and so it's something we need to think about. OODAL stands for observe, orient, decide, act, and it is a cycle. This was developed by an Air Force military strategist John Boyd, and he developed that for thinking about dog fights. Pilots in a dogfight is continually going through this oddle loop in his mind: observe, orient, decide and act. Right? This is the process of collecting, evaluating, and then doing. And this type of process is widely applied in any real time adversarial situations. You'll see articles that talk about not only airplane dogfights, but strategic military planning, business competition, anything else.

By definition, it's an iterative process. Someone in this kind of situation is continually going through loops in their head. And what Boyd observed is that speed is essential here, that if you can make your oddle loop faster than the adversaries, if you can get what the phrase uses inside the other person's oddle loop, then you have an enormous advantage. Right? You can respond effectively faster. Then he can react to your response. There is some good writing about applying this to at the cybersecurity and response. Their papers I may recommend, just google the term and wondering around a bit.

What I think we need, the reason I like this framework is that it gives us a way at discussing affected tools for instance response. So, really, what's this talking is that at this point, there is a plea for tools. We need good IR tools to facilitate all the steps, and we can break them down. The first step is observe, knowing what's happening on our networks in real time. So, that's real time threat detection from IDS; that's log monitoring, log analysis tools, network performance analysis tools; network management tools; physical security information; pretty much everything. We may be able to get all that data in a place where it can be monitored in real time, both before during an attack.

Oreint, understanding what this information means in contexts, and context is critical in any response. So, the contexts of the organization: what's happening in the company at the time, in the context of the greater Internet community, you know, what kind of malware is out there, what kind of zero days we are just seeing, what kind of geopolitical situation is going on. Right? Are there some new vulnerability that was just discovered are announced? Is your organization rolling out a new piece of software? Are they planning layoffs? Is there a merger? Has your position seen attacks from this IP address before? Has it never been open up to a partner? Everything again,

everything in the database, from the news, from intelligence feeds to the rescue of the organization. Just ways to put what's going on in contexts.

Third, decide, figuring out what to do in the moment. This is actually hard. Who has the power to make a decision? How do they make the decision? What sort of executive input is required? Is their marketing input? Is their PR input? Is their legal input? How do you justify the decision? Because after the fact he made whole of in front of some investigative body, either in your company or some lawsuit, to justify why you did what you did. That's all parts of the decision process.

And then act, being able to make changes quickly on the network. And again, here a lot of organizations found out because the people in the IR team might not be authorized to make changes all the way over there. They might not have the authorities. And we won't know what authorities they need until it all starts, acquiring product access and continual training. We need tools for all these things. We need tools that are powerful, flexible, intuitive, tools that aid people. And we don't love them. This isn't one thing, this is a whole ecosystem of incident response, products and services that do these things. Response is getting more important for a lot of reasons: attacks are more sophisticated, the regulatory environments are getting more complicated, mitigations are much more common, geopolitical factors are major, and again, organizations understand on prevention.

And the neat thing in the reason I'm really optimistic about this next few years is that IR software is not going to be like the rest of the securities offered, that the Y requirements, all the stuff I just listed, none of them are those non-functional requirements. They are all stuff the products and services have to do. And this means the good stuff is gonna beat out the mediocre stuff. And we as engineers need to start building the good stuff, because it's important. I've started doing this at a company called Three Systems. I'm trying to build a management platform to coordinate instance response. That's just one piece of it. The thing important is the core one, but lots of things have to feed into it. It has to be into a lot of things, it has to work together. The goal here is to bring people, process and technology together in a way that hasn't been done before, in a way that is going to mirror less IT and more things like generic crisis management. We have a lot to learn from other disciplines that have been doing this sort of thing for decades. And this is how we're gonna defend against threats, this is what's going to work.

So, that's how we take questions, or not, because that seems odd. As to the way this works, one person has to raise his hand, and then everyone else will. So, someone sort of has to be the guinea pig.

You know, I don't know, I mean, people come in under-investing for a long time and there've been lots of frameworks. I don't know how well that's gonna make a change. I think fundamentally, we will always under-invest. It is much more closely effective to respond to the attack than to invest before the attack. When you get credit for doing something, its focus, its target people are impressed. We will under-invest always and after the fact, try to fix things. Think of something very fundamental about us as people, and what are we gonna do? So, I don't have a lot of hope that anything will change.

I don't think you can automate the response. It's too strategic. It's not like a patch, that you just

install the patch. It depends so much on human things, defense or cooperation. You can automate some other things, the getting ins and outs. Getting all the data, you could automate. And when you figure out what to do, you can automate doing it, but you still need the step of analyzing and figuring it out that requires human brain. So, pieces can be automated and make sense to do. But, the actual process of IR will always require a human team. Now, companies might outsource that team. There are lots of companies out there that will handle your IT infrastructure, including instant response. But they're gonna have to court with you because that's your business. So, no, I don't think we can pull humans out of the loop here. When we invent an AI, maybe. But until then, no.

The questions about striking back. I'm really not favor strike back. I mean vigilante justice is not work well in our society. You know, that being said, I think we are going to see more about it because companies are getting fed up. But you are gonna have attackers win a match of their origins, you know, all attacks via his network, in a strike back against him. That's great. We have a lot of trouble targeting attacks back. We can identify attacks sometimes, but it takes weeks and months. That grows great reporter Mandiant take a while to generate. You are not going to figure out who attacked you or what in milliseconds which what you need to strike back. So, no, I do not think that's going to the answer. I think it's a dangerous trend. I'm really not favor it because it's too easy to get wrong and to go after innocence.

The question about government requirements in response. There's a lot of questions about the government's requirements for security in general. I think that is coming, especially in industries that matter. Just like their government requirements for food safety, that we're gonna see government requirements for data safety. It will depend, you know, US forces, Europe politics. But that sort of thing and minimal required security is something that's very common in other areas, and they will get IT eventually. I'm not sure it's a good thing like you. But I do think it's coming and I think the era of government saying "you know, let industry handle it will work out okay" is coming to an end. And you know there will be more government involvement. At what level remains to be seen exactly, it was gonna be government takeover or security, it's gonna be tax incentives, it's gonna be sort of like FDA or FTC, penalties and rules depend on politics. But I do think more government involvement is coming.

I have seen response companies are doing is very well. They tend to come from industries that had incidents way before computers. So, you know oil and gas, companies deal with hurricanes. Incidents happen and they are good at convening teams, ad hoc, and figure out what to do and doing it. And IT, it's just the tech add on to a much broader type a system. So, yes, there are a lot of places that we in IT can learn from who'd been doing this since forever, just without the same level of tech. And again, I think it's a really good thing, which will see a lot of good cross fertilization between.

Questions about cloud companies and how they seek security. It's interesting to watch. You know, the bigger cloud companies, their security model is trust us. If you go to, you know, you outsource email to Google and you go to Google and say "you know, we need to order our email system". They say no and if you say "well, we are gonna use you" and they say ok. So, their model is take it or leave it, and they are big enough to do that. Some smaller companies do have some ability to audit. I think what's gonna happen is some kind of waterfall model. The way this

matures is that you host your infrastructure to make this up on Rackspace. Rackspace will have it and audit it. You can get a copy of and staple in your audit. And then you hand that to the people who are out on this stuff to you, and they staple in their audit. And I think that's the way it will go. I'll take a while to get there, but I see no other way to make this work. There aren't any audit requirements, but no companies allow someone else to audit their stuff. But they will allow give you the piece a paper saying "we've been audited, this is the result". So, you can use data satisfy your own regulators. I think this is coming, and no other way that can work.

So the question about incident response. How could an enterprise compete with a threat after superior resources? Probably can't. The attacker's going to get in. The question is what happens afterward, and it's not always a matter of who has the more money wins. It has to do with our risk aversion, has to do with the legal environment. It's often "I can't compete with a hacker that's better than me" by calling the police. Right? That's a way I could temporarily get some more resources. So, we have a lot of negligence society for dealing with attackers that are more skilled, scarier, bigger than us. We wish to make them apply here. But, in general, I think an attacker that has more resources is going to get in. The question is now how do we can kick them out, how do we regain security, how do we oodle resilient against that. That's the whole notion of response. We are responding because the attacker has broken into our network, not responding to a potential, we are responding to an actual. And you know, there are a lot of things we can do without a matter of saying "well, they are gonna get in, so we are done". It's a matter containing some other damages.

By resilient, I mean several things: how do we maintain, how do we mitigate the threat, how do we reduce the amount of damages the bad guy does when he is in, survivability, how do we survive, how do we make sure that we don't just fall over dead, how do we recover, how do we kick him out and regain security. This can be really difficult. And how do we adapt, how do we continually improve ourselves to make our security better. So, I think a resilience as a whole kind of basket. Again, it's a different Y requirements to make us secure even in the face of the bad guys are gonna get in. And there are a lot of examples. As a species, we are resilient to diseases. Disease will kill some of us but won't kill all of us, and we have genetic diversity that is the security mechanism by which we are resilient to diseases. That's not actually a good strategy for IT. It's not gonna be good to say "well, look you know ten percent of you will be caught by this virus, and the rest of us will survive". That's kind of lousy. But, you know, that's what species do. So, I think of a broad basket of ways that we can build security, that can deal with the fact that there are threats that were petrified.

You know, I think bounty programs are interesting and useful. I'm not sure. I want to help more. Unfortunately, both the military market and the black market pay more than the bug bounties. I think it's attractive to people. They certainly help. Now I like seeing it that companies are taking this stuff seriously. But you know we're just seeing more and more cyber weapons and arms manufacturers finding bugs and then not turning them in because they can make more money selling them to governments around the world. So, I like the programs. I think they're good. I'm just not really holding out hope that they are gonna make that much difference. It's frustrating.

The question about prospect theory. How do we help to change the minds of people? This is hard. Right? The way you overcome psychological biases in general is to know about them and compensate. You know that you are risk-averse when it comes to gains and resilient when it comes

to losses. You can notice the behavior in yourself and compensate for it, just like there's a whole lot of psychological biases the casino floors playing on. If you know them, you can walk by those tables, look at them and say “well, that's a tax on people who don't know math, keep going”. So, the way we overcome them is by knowing them. This is hard. You know, the fear of terrorism. There is an enormous number of psychological biases that terror plays on, that we as a country has fallen completely for. You know, it's talking about them that gets us to think about them and hopefully, I'll get beyond them. It is possible. And it’s not just IT. Right? This is people trying to sell insurance, burglar alarms. Yes, anyone that buy burglar alarms are those after they've been robbed or after their neighbors been robbed. That's when they buy them, that’s where it goes.

A false positive does kill a lot of these systems. We're getting better at that. That’s detection. Detection still has a lot of room for good technology. Other response can be what you do. And when we talk about response, I mean the specifically the ways we need to clear false positives quickly. I’ll give you two examples. One is airport security. You walk through the metal detector, goes off, and this screen are converted quickly, figure out what's going on. If it's a false positive, they will learn it quickly. On the other hand, when the NSA sends a tip to the FBI, they say that 10,000 alarms are out of the 11,000. It took hundreds of man-hours to clear every one of those false positives. They were much more expensive. So, the trick really is a fast secondary test that lets you clear the false positives. And if you can do that, then you can deal with a much faster and less annoyer primary test. This is basically how we deal with medical tests. So, that’s the thing we need.

So, thank you very much. I'll be here. I'm happy to talk, sign books.