电子废弃物情境下的用户信息安全保护动机研究*

陈昊[1]，吕途[1]，张嵩[1, 2]
（1. 青岛大学商学院，山东 青岛 266061；
2. 青岛大学质量与标准化学院，山东 青岛 266061）

摘 要 未经妥善处理的电子废弃物中往往存储有海量私密信息。一旦信息泄露，可能导致身份盗用、财产损失，甚至危及国家安全。从行为学视角整合社会学习理论和保护动机理论，构建个体电子废弃物持有者信息安全保护动机要素模型。结构方程模型检验结果表明：信息安全意识是风险评估与应对评估产生的重要前因；感知威胁和自我效能是影响保护动机产生的关键因素；感知有效性负向影响保护动机，并且响应成本正向影响保护动机。

关键词 电子废弃物，隐私安全，保护动机理论，安全意识，响应成本

中图分类号 C931.6；G353.1

1 引言

电子废弃物是被持有者废弃且不会再次使用的电器或电子设备及其部件[1]。信息技术升级频率的加快带动了电子设备的快速更新换代。2019 年全球产生的电子废弃物总量达到了创纪录的 5 360 万吨，五年内激增 21%[2]。电子设备信息存储性能的改善与应用场景的扩展，使得多类型的海量信息可以通过电子设备存储和传输。电脑、手机、U 盘、智能设备和物联网设备等在正常使用时通常存储大量个人隐私信息、商业机密或政府机要文件。随着这些设备被废弃，且没有经过妥善的数据清理或设备处理，私有信息将可能被其他人员获取（直接读取或恢复数据），从而带来隐私信息安全隐患和财产损失[3, 4]，甚至威胁国家安全[5]。

近年来，个人隐私信息安全研究受到广泛关注[6]，学界就信息安全保护机制进行了行为学层面的深入探讨。人们普遍关注各行各业中正在使用中的电子设备的隐私安全及其保障措施使用，如关注医疗数据隐私泄露[7]和政府数据开放平台的隐私安全[8]，并尝试讨论通过安装防护软件保障计算机安全[9]、使用安全技术来保障手机安全[10]，以及电子设备失窃可能导致的信息安全危害及其补救[11]等。然而，对于电子废弃物，人们普遍认识到它们对于环境和健康的危害性，却忽视了其潜在的信息安全风险。调查显示，54%的废旧手机中含有诸如邮件列表、银行账户等隐私信息[12]，给身份盗用和信息诈骗带来可乘之机。

废弃物情境下的隐私信息安全面临着安全意识匮乏和忽视保护的问题。人们对废弃物情境下的隐私信息安全风险和其潜在的不良影响缺乏意识，从而无法从认知上重视和关注该安全风险。此外，废弃物中的隐私信息处置面临着技术困境，而人们往往缺少必要的安全知识和处置措施。例如，面对无法开机的废旧电子设备，人们多数不知道应该如何清理存储其中的隐私信息。当前研究缺乏电子废弃

* 基金项目：教育部人文社会科学规划基金项目（20YJC630003）、山东省高等学校“青创科技计划”（2019RWG031）。
通信作者：张嵩，青岛大学质量与标准化学院教授、博士生导师，E-mail：carolezh@sina.com。

物信息安全保护行为的探讨，相关保护机制有待建立。本文以此为契机，从设备持有者的立场，认为在废弃电子设备前进行有效的信息清理和设备处理是保障隐私信息安全的重要举措。研究整合社会学习理论和保护动机理论，构建保护电子废弃物信息安全的动机要素模型，揭示影响电子废弃物持有者实施信息安全保护行为的关键要素和影响机制。研究结论为电子废弃物信息安全管理提供理论证据，为政策制定与实践提供支持。

2 理论基础与研究假设

2.1 保护动机理论

保护动机理论（protection motivation theory，PMT）[13]认为动机产生是自身对威胁评估和应对评估的预判认知的结果。威胁评估包括感知严重性和感知易感性，分别用于评判威胁可能造成的后果严重程度，以及产生负面影响的可能性概率。应对评估解释了应对措施对威胁的处置有效性（感知有效性），揭示了应对这些威胁所需的能力（自我效能），以及实施应对措施所需的成本（响应成本）。如果人们相信应对措施是有效的、低成本的，并且他们有能力或信心去实践，那么他们会愿意采取应对措施。威胁评估和应对评估的建立依赖于外部环境信息的输入，如口头交流、可见的学习，或者源于他人经验[13]。Vance 等[14]的研究识别了源于先前经验的习惯对于保护动机认知评估的作用，Tu 等[11]则揭示了风险响应相关的知识、社会影响和威胁相关的经验对于保护动机认知评估的作用机制。由此，保护动机理论揭示了一个基于外部信息的风险决策评估过程。该理论被广泛应用于信息安全行为研究领域，探讨安全技术的采纳动机[15, 16]和预测组织与个体的信息安全行为[17, 18]。

保护动机理论认为风险评估包括感知易感性和感知严重性[13]，且风险评估认知通常是感知易感性和感知严重性共同作用的结果[19]。据此，本文将感知威胁作为风险评估的基本构念，指代个体对于威胁的易感性和严重性预判认知。根据保护动机理论，当个体认为自己容易成为威胁攻击的目标，且一旦遭受威胁会产生严重性的后果，那么保护动机随之产生。风险评估过程是安全保护行为的必要环节[20]。当电子废弃物持有者认为自己持有的废弃设备成为信息窃取者的攻击目标的可能性较高，并且信息泄露带来的影响严重性程度较高，那么他们会产生保护动机来实施保障信息安全的行动，以降低风险的发生概率。由此，提出假设：

H_1：感知威胁正向影响保护动机。

应对评估包括感知有效性、自我效能和响应成本[13]，通过效能成本分析驱动保护动机的产生。感知有效性是指对响应措施是否能够有效应对威胁的判定[21]。已有研究发现，感知有效性对安全技术的采纳有着积极的影响作用[9, 21]，响应措施越有效，越能够激发人们采取该措施来降低安全风险。同样，电子废弃物持有者通过有效的数据清理措施，如使用擦除工具清理数据或物理损坏（砸坏、消磁等）的方法处理废弃设备等，能够最大限度地避免信息泄露，因此人们倾向于采用自认为最有效的方法来保护废弃设备中的信息安全。由此，提出假设：

H_2：感知有效性正向影响保护动机。

自我效能是指采纳响应措施所需要的能力和信念的认知[22]。已有研究认为，高程度的自我效能是驱动个体采取 IT 安全行为的重要动力[9, 23]。由此，电子废弃物持有者的自我效能越高，即他们采取响应措施的能力和信心越高，越容易激发其采取这些措施来保障废弃物设备中的信息安全的意愿与动机。由此，提出假设：

H_3：自我效能正向影响保护动机。

响应成本是指采纳和实施响应措施所需要付出的成本，包括耗费的时间、金钱、努力，由此产生的不便、遇到的困难、复杂性、不愉快和可能带来的其他消极后果等[15, 24, 25]。已有研究发现响应成本与保护意愿呈负相关关系，即人们采取响应措施来保护信息安全的意愿随着响应成本的增加而降低[9, 10]。本文研究环境下的响应成本更加侧重于在采纳和实施响应措施时付出的努力和遇到的困难。电子废弃物持有者操作数据清理工具需要学习理解关键术语并掌握它的操作使用，在此过程中需要付出努力甚至会遇到困难。人们通常更愿意花费更少的成本来进行行为决策[9]。一旦人们认为自己无法掌握或者对于响应措施的实施有困难，那么他们将放弃采取这些措施。由此，提出假设：

H_4：响应成本负向影响保护动机。

2.2 社会学习理论

社会学习理论（social learning theory，SLT）认为个体行为是由认知和环境共同作用的结果[26]。该理论强调可见的外部刺激与环境反馈是认知形成的基础，并通过认知加工评估作用于个体的行为动机。社会学习理论的关键环节是学习[26]。个体不断地通过一系列可见的外部线索，如周围人的经验，或观察其他人的行动和反应结果，来形成并强化对于特定事件的看法和态度，继而模仿或借鉴他人的积极经验来处理应对自身遇到的同类或类似事件。学习过程的最终目的是通过外部信息的输入进行认知加工来形成自己的认识，从而做出理性的行为判定。社会学习理论被用于探讨计算机闲散行为[27]、计算机骚扰行为[28]与信息安全行为[29]等。在本文的信息安全情境下，个体对电子废弃物中潜在的信息安全风险的认知来源于社会学习的过程。通过一系列的外部信息源，如社会媒体和同事或亲朋的经验习得而获得外部线索信息。这些信息通过自身的认知加工，最终形成对电子废弃物情境下针对潜在的信息安全风险的知识，即信息安全意识。外部环境的关键作用隐含在信息安全意识的习得过程之中，是信息安全意识产生的必要前提和不可或缺的条件。

对电子废弃物的数据清理和设备处置与其持有者的信息安全意识和行为有着密切的关联，信息安全意识越低的设备持有者越容易低估信息安全风险，从而疏于应对。因此，从行为学视角出发探讨设备持有者保护电子废弃物信息安全意识，了解该保护行为决策发生的关键性要素显得尤为必要。根据已有研究[30]，将信息安全意识定义为个体对电子废弃物情境下信息安全潜在问题与后果的全部知识与理解，包括个体对电子废弃物环境下信息安全重要性的理解程度，以及使用潜在解决方案的认识程度等。

信息安全意识的作用路径可以用创新扩散理论[31]描述的决策过程框架，即“知识–说服–决策”链条进行解释。信息安全意识被视为知识，保护动机要素被视为说服的过程，保护动机作为决策的结果。基于这个思路过程，个体一旦获得对电子废弃物环境下的信息安全问题及潜在后果的知识，他们会综合评估自己可能受到的威胁的可能性和严重性，以及应对的途径和方法，继而刺激自身的保护动机决策的生成。据此，人们的信息安全意识越强烈，越容易知觉到自身可能遭遇的潜在信息安全威胁。由此，提出假设：

H_5：信息安全意识正向影响感知威胁。

已有研究发现通过信息安全知识与经验的培养，可以提升个人对信息安全风险的应对[15]与信息安全技术的采纳使用[32]。因此，信息安全意识较高的个体倾向于通过采取安全保障措施，如采用安全技术解决方案来保障信息安全，并且信息安全意识越高，个体知觉到的解决方案有效评价越客观[23]。由此，提出假设：

H_6：信息安全意识正向影响感知有效性。

电子废弃物环境下的信息安全保障有其情境特殊性。电子废弃物环境下的信息安全问题的解决涉

及两个部分，即对内有信息的彻底清理和对电子设备的正确处置。只有完全清理掉内置数据，同时将设备进行安全处置，确保已经清理掉的内置数据不被再次恢复和读取，才算完成了安全保障行为。进行正确的设备处置和数据清理需要专业的知识来进行，对于绝大多数普通用户来讲，这些专有知识不见得人人都能够掌握和操作。特别是在诸如格式化和恢复出厂设置等处置方案被证实无法进行彻底数据清理[33]的情形下，人们了解到的电子废弃物环境下的信息安全知识越多，越可能会感觉到作为普通用户在风险规避和处置上的无能为力。例如，当无法正常开机使用的电子废弃物中存有重要信息时，普通个体用户多数不知道该如何处置清理内置信息，由此几乎没有办法去保障信息安全。由此，提出假设：

H_7：信息安全意识负向影响自我效能。

电子废弃物环境下的信息安全保障并非易事，人们需要付出必要的努力来学习专业知识，并掌握和应用处置方案。在这个过程中也必须要克服诸多困难，如普通用户因为知识匮乏和理解力差异，对信息安全专业知识的理解和掌握困难，应用处置方案过程中的操作困难，等等。当高信息安全意识的个体对电子废弃物隐私安全的危害知晓得越多、对现行解决方案了解得越多，那么他们越能够知道应对电子废弃物信息安全问题可能要付出更多的努力和克服更多的困难去寻找行之有效的解决办法才能实现信息安全保障。因此，信息安全意识高的个体越能够了解实施安全保障措施的响应成本。由此，提出假设：

H_8：信息安全意识正向影响响应成本。

综上，整合保护动机理论与社会学习理论建立研究模型，如图 1 所示。

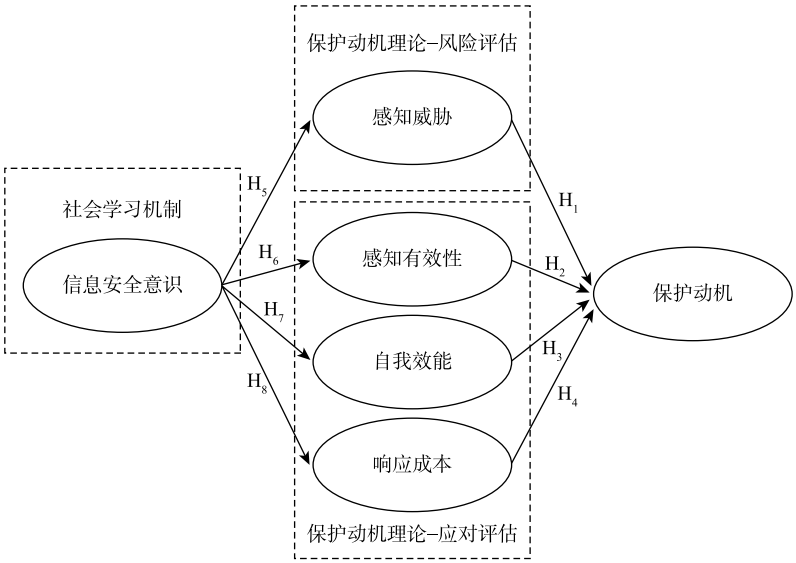

图 1 研究模型

3 研究方法与数据分析

3.1 量表设计与数据收集

大多数量表测度项来自已有文献，并针对研究情境进行了适当修订。保护动机的测度项设计参考电子废弃物的实际处理，从信息清理和设备处理两个层面来测度。其中，信息清理是指通过擦除存储

在设备中的信息的方式来确保无（重要）数据残留在设备中或数据难以被读取和恢复。设备处理是指通过物理损坏（砸坏、消磁等）手段确保数据不被读取和恢复。采用 Likert 五级量表进行刻度，考察被试对测度项的基本观点和看法。其中，1~5 分别代表从完全不同意到完全同意的态度变化。量表初步开发完成之后，通过专家小组讨论，根据反馈进行问卷调整，最大限度地保证量表的内容效度。

考虑到智能手机在各个年龄层的普遍使用及其快速的产品推新频率，选取废弃智能手机作为电子废弃物的代表。调查对象选取过去三年内有过更换智能手机经验的，以及未来一年内有计划更换现有智能手机的人群。依托专业调研网站，随机向符合条件的受访者推送调研问卷。在调研结束后，对回收的样本数据进行筛选，剔除前后矛盾、明显的恶意回答等不合格问卷后，回收有效问卷共计 301 份。回收样本分布特征参见表 1。

表 1　样本描述性统计

分类指标		样本量/人	比例	分类指标		样本量/人	比例
性别	男	145	48.173%	月收入/元	≤3 000	62	20.598%
	女	156	51.827%		3 001~6 000	147	48.837%
年龄	20 岁及以下	9	2.990%		6 001~10 000	75	24.917%
	21~30 岁	151	50.166%		>10 000	17	5.648%
	31~40 岁	108	35.880%	学历	高中及以下	26	8.638%
	41 岁及以上	33	10.963%		本科及专科	212	70.432%
工作类型	知识工作者	180	59.801%		硕博研究生	61	20.266%
	体力劳动者	101	33.555%		其他	2	0.664%
	其他	20	6.645%				

3.2　数据分析与研究结果

选用 PLS 偏最小二乘法和 SmartPLS 3.0 工具进行数据分析。为了排除共同方法变异的影响，通过 PLS 方法[34]检验共同方法偏差，发现主因子的平均解释方差为 0.635，方法因子的平均解释方差为 0.003，并且绝大多数的方法因子的题项载荷是不显著的。另外，采用 Harman 单因子法检测发现非旋转因子中最大单因子解释的协方差仅为 23.51%（＜50%）。两种方法检测结果均表明不存在共同方法偏差。此外，采用方差膨胀因子（variance inflation factor，VIF）检测变量之间的共线性是否存在。检测结果表明变量 VIF 值的范围为 1.044~1.494，均远小于 3.3 的推荐值，表明变量之间的共线性不存在。

1. 测量模型检验

首先对数据的信度进行检验，测量量表内容及各评价指标结果详见表 2。绝大多数构念的组合信度（CR）和 Cronbach's α 在 0.7 以上。感知有效性的 Cronbach's α 值非常接近 0.7，同样可以接受。由此，数据信度良好。其次进行效度检验。表 2 显示，平均变量萃取量（AVE）均大于 0.5，且根据表 3 交叉负荷和相关矩阵检验结果，所有测量项在各自的构念下的载荷值明显高于其他构念下的载荷值，且 AVE 平方根值大于所有的相关系数，表明数据的效度良好。此外，本文还采用 HTMT 矩阵（multitrait and multimethod matrix）检测区别效度。表 4 检测结果发现 HTMT 值均小于推荐值 0.85，表明区别效度良好。

表 2 测量量表和信度效度评价指标

构念及来源	测度项	因子载荷	AVE	CR	Cronbach's α
信息安全意识[30]	我通过新闻、互联网等了解到废旧手机存在信息安全隐患	0.846	0.683	0.896	0.846
	亲朋好友或周围的人谈论过关于废旧手机的信息安全问题	0.836			
	我了解废旧手机中潜在的信息安全问题的解决办法	0.810			
	我关注关于废旧手机信息安全问题的解决办法的新进展	0.813			
响应成本[9]	操作清理工具来清除废旧手机中的信息时有点麻烦	0.706	0.617	0.828	0.701
	应用清理工具擦除废旧手机中的信息需付出额外的努力（如需要学习清理工具的使用方法）	0.814			
	理解数据清理工具中涉及的专业术语或操作指令会有困难	0.830			
感知有效性[35]	我认为自己对保护废旧手机中的信息所做出的努力可以有效防止数据被窃取	0.821	0.624	0.832	0.698
	我认为自己对保护废旧手机中的信息所采取的措施可以有效阻止他人获取信息	0.806			
	我认为自己使用的防止废旧手机中的信息被恢复的举措对减少数据失窃非常有用	0.740			
感知威胁[35]	我的废旧手机很可能会成为他人窃取信息的目标	0.825	0.644	0.879	0.816
	我的废旧手机转手给他人后，数据信息有可能会被恢复	0.816			
	存储在废旧手机的信息可能会被泄露，因此隐私会被侵犯	0.805			
	废旧手机的信息安全问题很严重，应该被关注	0.765			
保护动机[35]	我打算采取措施擦除我的废旧手机中的数据文件	0.819	0.646	0.880	0.817
	我愿意采取措施清理我的废旧手机中的信息	0.810			
	我会妥善处置我的废旧手机以防止数据信息被他人获取*	0.775			
	我计划通过安全可靠的渠道来回收我的废旧手机以避免数据信息被他人获取*	0.811			
自我效能[35]	对我而言，采取措施来保护废旧手机中的信息很容易	0.768	0.643	0.879	0.815
	我有能力采取措施把废旧手机中的信息清理干净	0.834			
	我可以使用数据擦除工具来防止废旧手机信息被他人获取	0.821			
	我能够采用数据保护措施来防止废旧手机信息被他人恢复	0.782			

注：加*代表该测度项为自己开发

表 3 区别效度检验结果

构念	信息安全意识	响应成本	感知有效性	感知威胁	保护动机	自我效能
信息安全意识	**0.827**					
响应成本	0.270	**0.785**				
感知有效性	−0.074	0.306	**0.790**			
感知威胁	0.166	0.415	0.354	**0.802**		
保护动机	0.132	0.627	0.260	0.535	**0.804**	
自我效能	−0.162	0.176	0.442	0.039	0.257	**0.796**

注：黑体数字为 AVE 的平方根值

表 4　HTMT 检测结果

构念	信息安全意识	响应成本	感知有效性	感知威胁	保护动机	自我效能
信息安全意识						
响应成本	0.344					
感知有效性	0.124	0.446				
感知威胁	0.197	0.545	0.469			
保护动机	0.158	0.567	0.342	0.652		
自我效能	0.201	0.230	0.581	0.090	0.306	

2. 假设检验

假设检验的结果见图 2。模型的累计解释总体方差变异为 54.6%，其中控制变量解释总体方差变异为 2.9%。研究发现知识劳动者比体力工作者更倾向于产生电子废弃物情境下的信息安全保护动机。

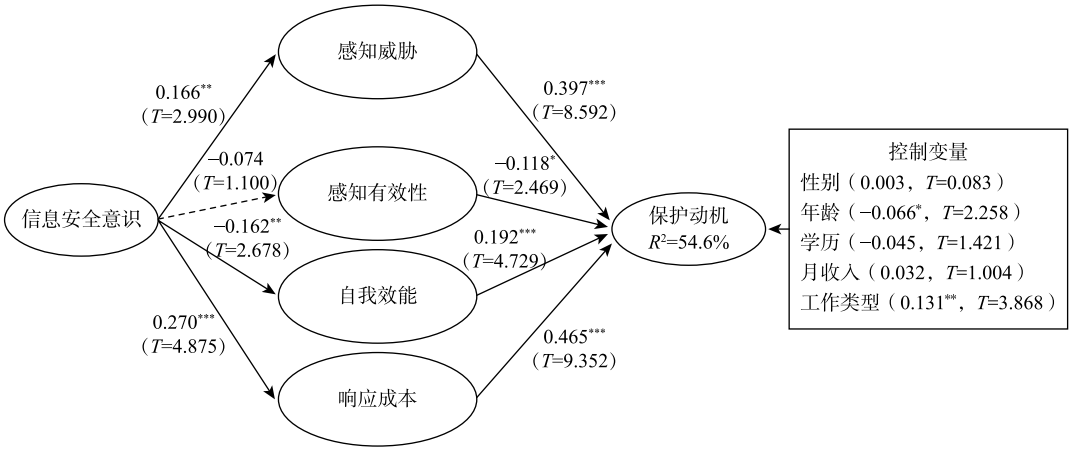

图 2　假设检验结果

***表示 $p<0.001$，**表示 $p<0.01$，*表示 $p<0.05$；虚线表示路径不显著

感知威胁正向影响保护动机，H_1 得到支持。该研究结论与已有研究结论相同，均认为感知风险是激发保护动机的重要因素。电子废弃物持有者感知到的信息安全风险越高，越容易产生采取响应措施来保障信息安全的行为意愿。

感知有效性与保护动机之间的路径系数负向显著，与原假设相反，H_2 不被支持。已有研究普遍认为越是有效的响应措施越容易驱动保护动机的产生[9, 10]。与 Vance 等[14]的研究结论相同，本文没有发现感知有效性会降低保护动机。表 3 显示感知有效性与保护动机之间的相关系数为正（r=0.260），但假设检验结果发现两者之间的路径系数为负（β=−0.118）。为了解释这一变化，首先检验共线性。结果显示 VIF 为 1.494（＜3.3），故共线性不存在。其次，检验压抑效应（suppression effect）[14, 36]，发现感知威胁是感知有效性的压抑变量（suppressor variable）。单独检测感知有效性与保护动机间的路径系数显著为正（β= 0.311，$p<0.001$），这与保护动机理论的主旨相一致。

自我效能正向影响保护动机，H_3 得到支持。与已有研究结论相同，认为自我效能越高，越容易产生保护动机。电子废弃物持有者采取响应措施的能力和信念越高，其采取这些措施来保障信息安全的意愿越强。

响应成本与保护动机间的路径系数显著为正，与原假设相反，故 H_4 没有得到支持。通常，人们在理性思维的指引下会放弃高成本的响应措施，如张晓娟和李贞贞发现响应成本负向影响智能手机

用户的信息安全行为意愿[10]。然而，本文却发现响应措施的高成本反而成了驱动电子废弃物持有者采取该措施保障信息安全的驱动力要素。已有研究中对响应成本与保护动机或保护行为之间的关联同样发现了与原 PMT 构念关联有所差异的结论，如响应成本对智能设备用户失窃情境下的安全保障行为不产生影响作用[35]。本文发现的结论与 Barlette 等的研究结论相似，他们的研究认为响应成本对领导者们（CEOs）的信息安全保护行为产生积极影响作用[37]。电子废弃物环境下，处置电子废弃物以及清理废弃物中的常见的手段，如格式化或者恢复出厂设置等方式并不能完全清除数据[33]，这无疑增加了个体的响应成本。因此，保障电子废弃物环境下的信息安全成为一项有难度、有挑战的任务。组织行为学文献认为，困难并非都是阻碍绩效的障碍，很多困难被认为具有挑战性，更容易激发员工的斗志[38]；心理学和信息系统研究文献也发现类似的结论，即人们更倾向于付出努力来挑战有一定难度的任务和工作，因为复杂任务比简单任务有更多的挑战性[39]。也就是说，这种困难性反而会促进个体对信息技术的积极态度，并提升其采纳的可能性[40]。结合研究结论，对于电子废弃物持有者来说，一旦他们认为自己成为信息安全事件的潜在受影响群体，那么他们愿意付出更多的努力、挑战更多的困难来保障信息安全，表现出“迎难而上”的行为特性。从这个层面讲，响应成本与保护动机之间的正向关系是合理的。

信息安全意识正向影响感知威胁，H_5 得到支持；信息安全意识与感知有效性间的路径系数不显著，H_6 没有得到支持。H_6 没有得到支持的原因可能与电子废弃物信息安全情境的特殊性有关。由于现有解决方案如格式化等方法在应对电子废弃物信息安全问题上的局限性[33]，人们对风险威胁了解得越深入以及对现有应对方案了解得越多，可能越容易产生对这些解决方案的有效性的质疑。此外，信息安全意识负向影响自我效能，正向影响响应成本，H_7 和 H_8 得到支持。上述两个研究结论与已有研究发现的信息安全意识正向影响自我效能[41]、负向影响响应成本[23]不同，这可能是电子废弃物研究情境的特殊性所致。

此外，研究发现年龄和工作属性对保护动机的影响。与高龄人群相比，年轻群体对电子废弃物环境下的信息安全保护更具行动力，容易产生保护动机；与体力劳动者相比，知识劳动者对电子废弃物信息安全保护的意愿更强烈。

4 研究贡献与展望

本文有如下理论贡献。首先，引入电子废弃物环境这一新情境，开展针对电子废弃物持有者的信息安全保障行为的实证研究。已有研究针对组织情境下和个体日常情境下正在使用中的设备的信息安全问题[9, 10]以及电子设备失窃情境下的信息安全行为问题[11]进行了大量探讨，电子废弃物的信息安全问题缺少行为学研究领域的讨论。本文整合社会学习理论和保护动机理论，构建了电子废弃物持有者实施保护行为的动机要素模型，并验证了模型的解释度和有效性。

其次，揭示了信息安全意识对电子废弃物环境下个体保护动机评估的关键作用。基于风险的决策认知过程应该通过学习机制获取足够的正确知识来对风险和应对进行精准评估，而后才能做出正确的行为决策。研究展示了信息安全意识对威胁评估的正向影响路径，以及对应对评估过程的多向性影响过程，即对自我效能产生负向影响，对响应成本产生正向影响，对感知有效性无影响。信息安全意识相关的研究一方面展示了学习机制对信息安全风险评估过程的预测力，拓展了社会学理论在信息安全行为研究中的解释和应用；另一方面与组织情境下的员工信息安全行为相关的研究结论[15, 23]不同，本文对信息安全意识的差异化作用机制的展示揭示了电子废弃物这一特殊信息安全情境下个体心理动机与行为动机结果的路径过程。这些路径结论的发现提示未来研究对特殊信息安全情境下的行为研究的

关注。

最后，深化了对保护动机理论的理解。在电子废弃物环境下发现个体的风险应对评估要素与保护之间的新结论，即发现响应成本正向影响保护动机。该结论提示在理解特定环境下的个体信息安全行为时，不能完全按照既定的趋利避害思维来考虑问题，人们反而可能因为电子废弃物的难处置，而选择付出更多的努力和克服更多的困难，继而达成对信息安全的保障。该结论具有普遍的研究意义和价值，提示未来研究需要重新思考应对措施实施过程中遇到的成本及随后的行为决策。例如，已有研究往往认为当组织提供的解决方案的实施成本较高时，员工倾向于基于趋利避害的考虑，往往选择不去采用该解决方案来实施保护行为[9]。然而在组织面临新兴恶意计算机病毒攻击的时候，即便是潜在成本较高，也应该想尽办法对抗其可能带来的不利影响，而不是因为应对方法的困难或需要额外的努力就放弃对抗。

研究结论对于电子废弃物信息安全管理具有重要的参考意义和实践价值。首先，树立信息安全意识。应对风险的前提是能够有效地识别风险，因此对风险意识的培养显得至关重要。2016 年全国调查发现，超六成群众不能正确处置废旧手机，存在隐私泄露的可能性[42]。本文同样发现人们对如何应对电子废弃物信息安全风险缺乏足够的知识，以至于无法对风险应对进行准确评估。通过互联网、社会媒体等进行电子废弃物信息安全意识教育和知识传递是值得尝试的实践举措。其次，建立多渠道的电子废弃物处置机制，并通过服务或者设备硬件设计保护公众隐私。二手设备回收企业和电子设备厂商开始注意到电子废弃物信息安全问题，如华为提供以旧换新服务时开通了信息清理服务。对于社会公众而言，电子废弃物处置知识的缺失增加了其信息安全风险应对的难度。回收企业和电子设备制造商提供专业的信息清理服务无疑有助于公众安全地处置废旧设备以避免信息安全问题的侵扰，同时推动了废旧资源的合理配置。

本文尚存在一些不够完善和值得进一步探讨的地方。首先，选取废旧手机为代表探讨电子废弃物信息安全问题。此外，智能设备和物联网设备同样存储大量数据，如运动轨迹和位置信息、身体健康指标等隐私，未来可以针对新兴设备进行深入探讨。其次，企业和政府同样面临着废旧设备更换所带来的信息安全困境。通常，企业和政府的设备更换可能采取批量报废的形式，然而多数缺少电子废弃物管理准则，任何不严格的设备处置方式都有可能带来严重的信息安全隐患。未来研究可着眼于组织如何建立标准化可行性制度来规避电子废弃物的信息安全隐患。

参 考 文 献

[1] Baldé K，Wang F，Kuehr R，et al. The Global E-waste Monitor 2014[R]. Bonn，Germany，2015.

[2] Forti V，Baldé C P，Kuehr R，et al. The Global E-waste Monitor 2020. Quantities，flows，and the circular economy potential[R]. Unitar Scycle，2020.

[3] 中卫大城小事. 旧手机别随便卖！中卫市一男子刚卖完支付宝中 5000 元就没了！[EB/OL]. https://www.163.com/dy/article/FPD5VC2M0534MMOQ.html，2020-10-20.

[4] 广州日报. 破解旧手机盗刷 35 万余元，两男子获刑四年三个月[EB/OL]. https://news.dayoo.com/gzrbrmt/202011/10/158545_53644343.htm，2020-11-10.

[5] Robert M. Reportters find Northrop Grumman data in Ghana market [R]. IDG News Service，2009.

[6] 冯亚飞，严淳，胡昌平. 近 20 年来国内隐私领域研究的结构特征与热点透视[J]. 信息资源管理学报，2020，10（1）：65-74，101.

[7] 臧国全，张凯亮. 医疗数据隐私泄露容忍度的计量分析[J]. 信息资源管理学报，2020，10（4）：70-78，108.

[8] 杜荷花. 我国政府数据开放平台隐私保护评价体系构建研究[J]. 情报杂志，2020，39（3）：172-179.

[9] Liang H G，Xue Y J. Understanding security behaviors in personal computer usage：a threat avoidance perspective[J]. Journal of the Association for Information Systems，2010，11（7）：394-413.

[10] 张晓娟，李贞贞. 智能手机用户信息安全行为意向影响因素的实证研究[J]. 情报资料工作，2018，（1）：74-80.

[11] Tu Z L，Turel O，Yuan Y F，et al. Learning to cope with information security risks regarding mobile device loss or theft：an empirical examination[J]. Information & Management，2015，52（4）：506-517.

[12] Datashield. Consider the risks before you sell your old cell phone[DB/OL]. http://datashieldcorp.com/2014/02/05/selling-your-cell-phone/，2014-02-05.

[13] Rogers R W. Cognitive and psychological processes in fear appeals and attitude change：a revised theory of protection motivation[C]//Cacioppo J，Petty R. Social Psychophysiology：A Sourcebook. New York：Guilford，1983：153-176.

[14] Vance A，Siponen M，Pahnila S. Motivating IS security compliance：insights from habit and protection motivation theory[J]. Information & Management，2012，49（3/4）：190-198.

[15] Menard P，Bott G J，Crossler R E. User motivations in protecting information security：protection motivation theory versus self-determination theory[J]. Journal of Management Information Systems，2017，34（4）：1203-1230.

[16] Aurigemma S，Mattson T，Leonard L. Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications[J]. AIS Transactions on Replication Research，2019，5：article 3.

[17] van Bavel R，Rodríguez-Priego N，Vila J，et al. Using protection motivation theory in the design of nudges to improve online security behavior[J]. International Journal of Human-Computer Studies，2019，123：29-39.

[18] 甄杰，谢宗晓，李康宏，等. 组织内部员工的信息安全保护行为——基于 PMT 和 FA 整合视角的多案例研究[J]. 管理案例研究与评论，2017，10（2）：114-130.

[19] Liang H G，Xue Y J，Pinsonneault A，et al. What users do besides problem-focused coping when facing IT security threats：an emotion-focused coping perspective[J]. MIS Quarterly，2019，43（2）：373-394.

[20] Siponen M，Mahmood M A，Pahnila S. Employees' adherence to information security policies：an exploratory field study[J]. Information & Management，2014，51（2）：217-224.

[21] Johnston A C，Warkentin M. Fear appeals and information security behaviors：an empirical study[J]. MIS Quarterly，2010，34（3）：549-566.

[22] Verkijika S F. Understanding smartphone security behaviors：an extension of the protection motivation theory with anticipated regret[J]. Computers & Security，2018，77：860-870.

[23] Li L，He W，Xu L，et al. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior[J]. International Journal of Information Management，2019，45：13-24.

[24] Posey C，Roberts T L，Lowry P B. The impact of organizational commitment on insiders' motivation to protect organizational information assets[J]. Journal of Management Information Systems，2015，32（4）：179-214.

[25] Lee Y，Larsen K R. Threat or coping appraisal：determinants of SMB executives' decision to adopt anti-malware software[J]. European Journal of Information Systems，2009，18（2）：177-187.

[26] Bandura A. Social Foundations of Thought and Action：A Social Cognitive Theory[M]. Upper Saddle River：Prentice Hall，1985.

[27] Khansa L，Kuem J，Siponen M，et al. To cyberloaf or not to cyberloaf：the impact of the announcement of formal organizational controls[J]. Journal of Management Information Systems，2017，34（1）：141-176.

[28] Lowry P B，Zhang J，Moody G D，et al. An integrative theory to addressing cyberharassment in the light of technology-based opportunism[J]. Journal of Management Information Systems，2019，36（4）：1142-1178.

[29] Merhi M I，Ahluwalia P. Examining the impact of deterrence factors and norms on resistance to information systems security[J]. Computers in Human Behavior，2019，92：37-46.

[30] Bulgurcu B，Cavusoglu H，Benbasat I. Information security policy compliance：an empirical study of rational-based beliefs and information security awareness[J]. MIS Quarterly，2010，34（3）：523-548.

[31] Rogers E M. Diffusion of Innovations[M]. 5th ed. New York：The Free Press，1995.

[32] Dinev T，Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies[J]. Journal of the Association for Information Systems，2007，8（7）：386-408.

[33] Krumay B. The E-Waste-Privacy challenge：a grounded theory approach[C]//Schiffner S，Serna J，Ikonomou D，et al. Privacy Technologies and Policy. Berlin：Springer International Publishing，2016：48-68.

[34] Liang H G，Saraf N，Hu Q，et al. Assimilation of enterprise systems：the effect of institutional pressures and the mediating role of top management[J]. MIS Quarterly，2007，31（1）：59-87.

[35] Tu Z L，Yuan Y F，Archer N. Understanding user behaviour in coping with security threats of mobile device loss and theft[J]. International Journal of Mobile Communications，2014，12（6）：603-623.

[36] Petter S，Straub D，Rai A. Specifying formative constructs in information systems research[J]. MIS Quarterly，2007，31（4）：623-656.

[37] Barlette Y，Gundolf K，Jaouen A. Toward a better understanding of SMB CEO's information security behavior：insights from threat or coping appraisal[J]. Journal of Intelligence Studies in Business，2015，5（1）：5-17.

[38] van den Broeck A，de Cuyper N，de Witte H，et al. Not all job demands are equal：differentiating job hindrances and job challenges in the job demands-resources model[J]. European Journal of Work and Organizational Psychology，2010，19（6）：735-759.

[39] Tsang P S，Velazquez V L，Vidulich M A. Viability of resource theories in explaining time-sharing performance[J]. Acta Psychologica，1996，91（2）：175-206.

[40] Reynolds N，de Maya S R. The impact of complexity and perceived difficulty on consumer revisit intentions[J]. Journal of Marketing Management，2013，29（5/6）：625-645.

[41] Arachchilage N A G，Love S. Security awareness of computer users：a phishing threat avoidance perspective[J]. Computers in Human Behavior，2014，38：304-312.

[42] 中国青年政治学院互联网法治研究中心．中国个人信息安全和隐私保护报告[EB/OL]. http://www.thecover.cn/news/158619，2016-11-22.

Research on User Information Protection Motivation in the Context of E-waste

CHEN Hao[1]，LYU Tu[1]，ZHANG Song[1，2]

（1. School of Business，Qingdao University，Qingdao 266061，China；

2. College of Quality and Standardization，Qingdao University，Qingdao 266061，China）

Abstract Electronic waste（E-waste）devices without proper disposal may store an amount of private information. Once this information is disclosed，serious consequences such as identity theft，and property loss may occur，even such disclosure may endanger national security. From a behavioral perspective，this study integrates the social learning theory（SLT）and protection motivation theory（PMT）to build a research model to reveal information security awareness and motivation factors that influencing E-waste owner's information security behavior. PLS-SEM model testing results indicated that information

security awareness is the antecedent factor that motive E-waste owner's threat and coping appraisal；perceived threat and self-efficacy have direct effects on protection motivation；perceived effectiveness has a negative influence on motivation，and response cost positively impact protection motivation.

Keywords E-waste，privacy security，protection motivation，security awareness，response cost

作者简介

陈昊（1986—），男，青岛大学商学院副教授、硕士生导师，研究方向为行为信息安全管理、电子商务与 IT 行为等，E-mail：ch9569@qdu.edu.cn。

吕途（1988—），女，青岛大学商学院副教授、硕士生导师，研究方向为信息资源管理、创新创业等，E-mail：piko1210@126.com。

张嵩（1976—），女，青岛大学质量与标准化学院教授、博士生导师，研究方向为信息安全与隐私管理、社会化网络和商务数据分析、数字创业生态系统，E-mail：carolezh@sina.com。